MP/MP*

Colles de mathématiques

Rémi Coutens

550 EXERCICES CORRIGÉS

- Exercices de calcul
- Exercices de raisonnement
- Exercices avec questions ouvertes

ellipses

MP/MP*

Colles de
mathématiques

MP/MP*

Colles de mathématiques

Rémi Coutens

Sous la direction de François Pantigny

ellipses

Je remercie M. Pantigny pour ses relectures et ses pertinents conseils, mes collègues et amis MM. Devulder, Hoffbeck et Lucas pour leurs encouragements et leurs partages d'exercices. Ce livre doit également beaucoup à mon amie Emmanuelle Guillant qui n'aurait jamais imaginé qu'en déménageant à New York, elle y relirait les épreuves d'un livre de mathématiques.

Rémi Coutens

ISBN 9782340-054288

32, rue Bargue 75740 Paris cedex 15

www.editions-ellipses.fr

Avant-propos

En seconde année les interrogations orales n'engendrent plus d'appréhension. On sait que cette spécificité du système des classes préparatoires aux grandes écoles participe grandement aux progrès des étudiants. Cependant, cette seconde année est courte et à l'assimilation régulière du cours s'ajoute l'aspect de l'entraînement à l'oral. Néanmoins, de même qu'on ne se prépare pas à un marathon en faisant des marathons, un bon exercice pour l'oral d'un concours n'est pas forcément un bon exercice pour une « colle » au cours de l'année. C'est pourquoi même si certains sujets proviennent d'oraux de concours, ils ont parfois été modifiés afin de recentrer leurs questions sur un chapitre précis d'interrogation.

Dans l'objectif d'une préparation efficace, les exercices de ce livre sont classés en trois catégories :

- Les « exercices axés sur le calcul ». Souvent application quasiment directe du cours, ils ont pour objectif, via la pratique calculatoire, de vérifier la connaissance et la compréhension des notions du cours.
- Les « exercices axés sur le raisonnement ». Ces exercices demandant plus de recul, leur objectif est de renforcer l'assimilation des concepts.
- Les « exercices avec questions ouvertes ». Ces exercices amènent l'étudiant à avoir sa propre réflexion, à construire sa démonstration ou son contre-exemple selon les cas.

Plutôt que l'originalité ou la difficulté, nous avons privilégié des exercices qui nous ont paru formateurs. Néanmoins certains exercices, signalés par une ou deux étoiles, sont d'un niveau plus élevé.

Les corrections des exercices figurent après la liste des énoncés. Chaque exercice est entièrement corrigé parfois de plusieurs manières lorsque cela nous a semblé utile.

En espérant que ce livre contribue efficacement à leur préparation aux concours, nous adressons nos vœux de réussite aux lecteurs de ce livre.

Sommaire

Groupes 1

Exercices axés sur le calcul

Exercice 1 *Image par un morphisme de l'itéré d'un élément*

Soit G et G' deux groupes notés additivement. Pour $n \in \mathbb{Z}$ et $x \in G$, on désigne par nx l'itéré de x d'ordre n dans le groupe G.
Soit f un morphisme de G dans G'.

1) Montrer que pour $x \in G$ et tout $n \in \mathbb{N}$, on a $f(nx) = nf(x)$.
2) Montrer l'égalité précédente est encore vraie quand $n \in \mathbb{Z}$.
3) Que deviennent ces égalités en notations multiplicatives ?

Exercice 2 *Classique*

Soit f un morphisme de groupes de $(\mathbb{Q}, +)$ vers $(\mathbb{R}, +)$.
Montrer que pour tout $r \in \mathbb{Q}$, $f(r) = rf(1)$.

Exercice 3

Soit $\sigma \in \mathfrak{S}_9$ définie par $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 8 & 9 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}$.

1) Décomposer σ en produit de cycles à supports disjoints.
2) Déterminer la signature et l'ordre de σ.

Exercice 4

On rappelle que pour tout a réel, $b = \sqrt[3]{a}$ désigne l'unique réel b tel que $a = b^3$.
On munit $\mathbb{R}$ de la loi $\star$ définie par :

$$x \star y = \sqrt[3]{x^3 + y^3}.$$

1) Montrer que $(\mathbb{R}, \star)$ est un groupe abélien.
2) Montrer qu'il est isomorphe à $(\mathbb{R}, +)$.

Exercice 5 *Automorphismes intérieurs*

Soit $(G, *)$ un groupe. Pour $a \in G$, on note a^{-1} son symétrique pour la loi $*$ et τ_a l'application de G vers G définie par $x \mapsto a * x * a^{-1}$.

1) Montrer que τ_a est un automorphisme du groupe $(G, *)$ (c'est-à-dire un isomorphisme du groupe dans lui-même).

2) Vérifier que :

$$\forall a, b \in G, \quad \tau_a \circ \tau_b = \tau_{a*b}$$

3) En déduire que $\mathcal{T} = \{\tau_a, a \in G\}$ est un sous-groupe du groupe des permutations de G.

D'après Mines-Télécom

Exercice 6 *Centre d'un groupe*

1) Soit $(G, *)$ un groupe. On note :

$$Z(G) = \{x \in G \mid \forall y \in G,\ x \cdot y = y \cdot x\}.$$

Montrer que $Z(G)$ est un sous-groupe de G.

2) Montrer que l'ensemble des matrices de la forme $\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$ avec x, y et $z \in \mathbb{R}$ est un groupe pour le produit matriciel. Trouver le centre de ce groupe.

Exercice 7

On considère l'intervalle $I = [0, 1[$. Pour x et y dans I, on pose

$$x \star y = x + y - \lfloor x + y \rfloor$$

1) Montrer que $(I, \star)$ est un groupe abélien.

2) Résoudre l'équation $x \star x = 0$ d'inconnue $x \in I$.
En déduire qu'il existe un unique $d \in I$ qui soit d'ordre 2 dans $(I, \star)$.

3) Pour $n \in \mathbb{N}^*$, préciser, s'il en existe, les éléments d'ordre n de I.

Exercices axés sur le raisonnement

Exercice 8 *Classique*

Montrer que la réunion de deux sous-groupes est un sous-groupe si et seulement si l'un des deux sous-groupes est inclus dans l'autre.

Exercice 9

Soit $(G,*)$ un groupe d'élément neutre e et f l'application de G dans lui-même qui associe à tout x son symétrique x^{-1} pour la loi $*$.
Montrer que f est un automorphisme du groupe $(G,*)$si, et seulement si, le groupe $(G,*)$ est commutatif.

Exercice 10

On note $\mathrm{GL}_2(\mathbb{Z})$ l'ensemble des matrices carrées de taille 2 à coefficients dans $\mathbb{Z}$ dont le déterminant vaut 1 ou -1.

1) Soit M une matrice carrée d'ordre 2 à coefficients entiers et inversible.
   Montrer que si M^{-1} est à coefficients entiers alors $\det(M) = \pm 1$.
2) Montrer que $\mathrm{GL}_2(\mathbb{Z})$ est un groupe pour la multiplication.
3) On pose $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$.
   Calculer l'ordre de A, de B et de AB. Que peut-on en conclure ?

Exercice 11

Soit H et K deux groupes notés multiplicativement.

1) Soit h un élément de H et k un élément de K. On suppose ces éléments d'ordres finis.
   On note p l'ordre de h, q celui de k et $r = \mathrm{ppcm}(p, q)$.
   Montrer que (h, k) est un élément d'ordre r dans le groupe $H \times K$.
2) On suppose que H et K sont des groupes cycliques.
   Montrer que le groupe produit $H \times K$ est cyclique si, et seulement si, les ordres de H et K sont premiers entre eux.

Exercice 12

Soit G un sous-groupe fini de $(\mathbb{C}^*, \times)$.

1) Montrer que $G \subset \mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$.
2) Montrer qu'il existe $p \in \mathbb{N}^*$ tel que $G = \mathbb{U}_p$ (ensemble des racines p-ièmes de 1).

Exercice 13 ★★ *Groupes des éléments d'ordre fini de $\mathbb{C}^*$*

On note $\mathbb{U}_\infty = \{z \in \mathbb{C} \mid \exists n \in \mathbb{N}^*,\ z^n = 1\}$.

1) Montrer que $\mathbb{U}_\infty$ est infini.
2) Montrer $\mathbb{U}_\infty$ est un sous-groupe de $(\mathbb{C}^*, \times)$.
3) Montrer que $\mathbb{U}_\infty$ n'est pas engendré par une partie finie.

Exercice 14 ★★

Soit G un groupe fini noté multiplicativement, H et K deux sous-groupes de G.
On note $f\ :\ H \times K \to G, (h,k) \mapsto hk$ et :

$$HK = \{hk \mid h \in H,\ k \in K\}.$$

1) Quelle est l'image de f ? Déterminer le nombre d'antécédents par f que possède un élément de cette image.

2) En déduire que :
$$\mathrm{Card}(HK)\mathrm{Card}(H \cap K) = \mathrm{Card}(H)\mathrm{Card}(K)$$

Exercice 15 *Sous-groupe d'un groupe cyclique*

On désire établir que tout sous-groupe d'un groupe cyclique est lui-même cyclique : on introduit un groupe cyclique $(G,*)$, a un générateur de G et H un sous-groupe de $(G,*)$.

1) Justifier l'existence d'un plus petit entier naturel non nul tel que $a^n \in H$.

2) Établir qu'alors H est le groupe engendré par a^n.

Exercice 16

Soit $n \in \mathbb{N} \setminus \{0,1\}$ et $(G,*)$ un groupe de cardinal $2n$.
Soit A et B deux sous-groupes de G de cardinal n tels que $A \cap B = \{e\}$.

1) Montrer qu'il existe $c \in G$ tel que $A \cup B \cup \{c\} = G$.

2) Montrer que
$$\forall a \in A \setminus \{e\}, \forall b \in B \setminus \{e\}, \quad a * b = c$$
En déduire $n = 2$.

Exercice 17 ★

1) Soit f un homomorphisme de groupes de G dans G' et x un élément de G d'ordre fini p. Que peut-on dire de l'ordre de $f(x)$ dans G' ?

2) Trouver tous les morphismes de groupes additifs de $\mathbb{Z}/7\mathbb{Z}$ dans $\mathbb{Z}/15\mathbb{Z}$.

3) Trouver tous les morphismes de groupes additifs de $\mathbb{Z}/4\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$.

Exercice 18 ★

Montrer qu'il existe un multiple de 23 dont l'écriture décimale ne comporte que des 1.

D'après TPE Mines-Ponts

Exercices avec questions ouvertes

Exercice 19 *Caractérisation des groupes finis par le nombre de sous-groupes*

Soit $(G, *)$ un groupe.

1) Justifier que si G est fini alors G possède un nombre fini de sous-groupes.
2) Réciproquement, on suppose que G possède un nombre fini de sous-groupes.
   Tous les éléments de G sont-ils d'ordre fini ?
   L'ensemble G est-il fini ?

Exercice 20

Déterminer tous les morphismes de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.

Exercice 21

Soit n un entier naturel supérieur à 4 et $\sigma \in \mathfrak{S}_n$.
Existe-t-il un lien entre la parité de l'ordre de σ et sa signature ?

Exercice 22 *Classique*

Quels sont les morphismes de groupes continus de $(\mathbb{R}, +, \times)$ dans lui-même ?
Indication : Utiliser la densité de $\mathbb{Q}$ dans $\mathbb{R}$.

Corrections

Exercices axés sur le calcul

Exercice 1

On raisonne par récurrence.

1) Soit $x \in G$. Pour $n \in \mathbb{N}$, on a appelle $\mathcal{P}_n$ la proposition « $f(nx) = nf(x)$ ».
   Par définition, $0x = 0_G$ et $0f(x) = 0_{G'}$. Par ailleurs $f(0_G) = 0_{G'}$ car f est un morphisme.
   Donc $\mathcal{P}_0$ est vraie.
   Soit $n \in \mathbb{N}$. On suppose $\mathcal{P}_n$ vraie. On a alors :

$$\begin{aligned} f\big((n+1)x\big) &= f(nx + x) && \text{car } f \text{ est un morphisme} \\ &= f(nx) + f(x) && \text{d'après } \mathcal{P}_n \\ &= nf(x) + f(x) && \text{par définition} \\ &= (n+1)f(x) \end{aligned}$$

   ce qui montre que $\mathcal{P}_{n+1}$ est vraie.
   On a montré par récurrence que

$$\forall n \in \mathbb{N}, \quad f(nx) = nf(x)$$

2) Soit $x \in G$ et $n \in \mathbb{Z} \setminus \mathbb{N}$. Puisque f est un morphisme on a $f(nx) = -f(-nx)$.
Or $-nx = (-n)x$ et $-n \in \mathbb{N}$ donc $f(-nx) = (-n)f(n)$.
Finalement $f(nx) = -(-n)f(x) = nf(x)$.
On a montré

$$\forall x \in G, \forall n \in \mathbb{Z}, \quad f(nx) = nf(x).$$

3) En notations multiplicatives, on obtient :

$$\forall x \in G, \forall n \in \mathbb{Z}, \quad f\big(x^n\big) = \big(f(x)\big)^n.$$

Exercice 2

Soit $r \in \mathbb{Q}$. On choisit $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ tels que $r = p/q$.
En utilisant les images des itérés d'un élément par un morphisme (voir exercice 1) on a :

$$\begin{aligned} qf(r) &= qf\left(\tfrac{p}{q}\right) && f(qx) = qf(x) \text{ car } f \text{ est un morphisme} \\ &= f\left(q\tfrac{p}{q}\right) && q\tfrac{p}{q} = p = p \cdot 1 \\ &= pf(1) \end{aligned}$$

En divisant l'égalité par q, on obtient $f(r) = rf(1)$.

Exercice 3

1) En étudiant les images successives de chacun des éléments de $[\![1, 9]\!]$, on obtient :
$\sigma(1) = 3, \sigma(3) = 8, \sigma(8) = 1$. De même $\sigma(2) = 7, \sigma(7) = 2$.
Et $\sigma(4) = 9, \sigma(9) = 6, \sigma(6) = 5, \sigma(5) = 4$.
Donc

$$\sigma = \langle 1, 3, 8\rangle \circ \langle 2, 7\rangle \circ \langle 4, 9, 5, 7\rangle$$

2) • ***Signature***

La transposition $\tau = \langle 2, 7\rangle$ est de signature -1. Le cycle $c_3 = \langle 1, 3, 8\rangle$ est de signature $+1$ et le cycle $c_4 = \langle 4, 9, 5, 7\rangle$ est de signature -1.
La signature étant un homomorphisme de groupe, on a

$$\varepsilon(\sigma) = \varepsilon(\tau)\varepsilon(c_3)\varepsilon(c_4) = (-1) \cdot 1 \cdot (-1) = 1.$$

• ***Ordre***

Deux cycles de supports disjoints commutant pour la composition, on a pour tout $p \in \mathbb{N}$:

$$\sigma^p = \tau^p \circ c_3^p \circ c_4^p$$

La transposition $\tau = \langle 2, 7\rangle$ est d'ordre 2. Le cycle $c_3 = \langle 1, 3, 8\rangle$ est d'ordre 3 et le cycle $c_4 = \langle 4, 9, 5, 7\rangle$ est d'ordre 4.
On en déduit que l'ordre de σ est égal à $\mathrm{ppcm}(2, 3, 4) = 12$.

Remarque

On peut déterminer $\varepsilon(\sigma)$ en calculant le nombre d'inversions de σ. On trouve qu'il y a 22 couples (i,j) tels que $i < j$ et $\sigma(i) > \sigma(j)$. Donc $\varepsilon(\sigma) = (-1)^{22} = 1$. Mais il est plus rapide d'utiliser la décomposition en cycles. Quant à déterminer l'ordre de σ en calculant successivement σ^2, σ^3, etc., ce serait déraisonnable.

Exercice 4

1) • Montrons que la loi $\star$ est associative :
Soit x, y et z trois réels.

$$\begin{aligned}
(x \star y) \star z &= \sqrt[3]{(x \star y)^3 + z^3} \\
&= \sqrt[3]{(x^3 + y^3) + z^3} && x \star y = \sqrt[3]{x^3 + y^3} \text{ et } \left(\sqrt[3]{t}\right)^3 = t \\
&= \sqrt[3]{x^3 + (y^3 + z^3)} && \text{par associativité de } + \\
&= \sqrt[3]{x^3 + (y \star z)^3} && y \star z = \sqrt[3]{y^3 + z^3} \\
&= x \star (y \star z).
\end{aligned}$$

• De la même façon, la commutativité de $+$ entraîne celle de $\star$.
• Pour tout $x \in \mathbb{R}$, $0 \star x = x \star 0 = \sqrt[3]{x^3 + 0^3} = \sqrt[3]{x^3} = x$. Donc 0 est neutre pour $\star$.
• Pour tout $x \in \mathbb{R}$, $(-x) \star x = x \star (-x) = \sqrt[3]{x^3 + (-x)^3} = \sqrt[3]{x^3 - x^3} = \sqrt[3]{0} = 0$. Donc tout réel admet un symétrique pour $\star$.

On a montré que $(\mathbb{R}, \star)$ est un groupe abélien.

2) Notons $f : t \mapsto t^3$. On a

$$\forall x, y \in \mathbb{R}, \quad f(x \star y) = (x \star y)^3 = x^3 + y^3 = f(x) + f(y).$$

Donc f est un morphisme de groupes de $(\mathbb{R}, \star)$ dans $(\mathbb{R}, +)$.
Or f est bijective donc on a prouvé que $(\mathbb{R}, \star)$ est isomorphe à $(\mathbb{R}, +)$.

Exercice 5

1) Soit $a \in G$. Montrons que τ_a est un morphisme de groupes :
Soit x et y dans G.

$$\begin{aligned}
\tau_a(x) * \tau_a(y) &= (a * x * a^{-1}) * (a * y * a^{-1}) \\
&= a * x * (a^{-1} * a) * y * a^{-1} && \text{par associativité} \\
&= a * (x * y) * a^{-1} && a^{-1} * a = e \text{ (élément neutre)} \\
&= \tau_a(x * y).
\end{aligned}$$

Montrons que τ_a est une permutation de G :
Soit x et y dans G.

$$\begin{aligned}
y = \tau_a(x) &\iff y = a * x * a^{-1} \\
&\iff y * a = a * x \\
&\iff a^{-1} * y * a = x.
\end{aligned}$$

Donc tout élément de G a un unique antécédent dans G par τ_a. Donc τ_a est bijection de G dans lui-même.

Remarque
On peut même préciser que $\tau_a^{-1} = \tau_{a^{-1}}$.

On a montré que τ_a est un automorphisme du groupe $(G, *)$.

2) Soit a et b dans G. On a pour tout $x \in G$:

$$\begin{aligned}\tau_a \circ \tau_b(x) &= \tau_a\left(\tau_b(x)\right)\\ &= a * (b * x * b^{-1}) * a^{-1}\\ &= (a * b) * x * \left(b^{-1} * a^{-1}\right) \quad (a * b)^{-1} = b^{-1} * a^{-1}\\ &= \tau_{a*b}(x)\end{aligned}$$

Donc $\tau_a \circ \tau_b = \tau_{a*b}$.

3) En notant $\mathfrak{S}(G)$ l'ensemble des permutations de G, on vient de montrer que $a \mapsto \tau_a$ est un homomorphisme de groupes de $(G, *)$ dans $\left(\mathfrak{S}(G), \circ\right)$. Puisqu'on a un homomorphisme, l'image du groupe G est un sous-groupe de $\mathfrak{S}(G)$. Donc $\mathcal{T} = \{\tau_a, a \in G\}$ est un sous-groupe du groupe des permutations de G.

Remarque
$a \mapsto \tau_a$ étant un homomorphisme de groupes, on retrouve $\tau_a^{-1} = \tau_{a^{-1}}$.

Exercice 6

1) Par définition, $Z(G)$ est une partie de G.

- En notant e l'élément neutre de G, on a pour tout $y \in G$, $e * y = y * e$ donc $e \in Z(G)$.
- Soit x_1 et x_2 deux éléments de $Z(G)$. On a pour tout $y \in G$:

$$\begin{aligned}(x_1 * x_2) * y &= x_1 * (x_2 * y)\\ &= x_1 * (y * x_2)\\ &= (x_1 * y) * x_2\\ &= (y * x_1) * x_2\\ &= y * (x_1 * x_2)\end{aligned}$$

  Donc $x_1 * x_2 \in Z(G)$.
- Soit x un élément de $Z(G)$. On a pour tout $y \in G$, $x*y = y*x$. En multipliant à gauche et à droite par le l'inverse x^{-1} de x, on obtient $e*y*x^{-1} = x^{-1}*y*e$ donc $y*x^{-1} = x^{-1}*y$. Donc $x^{-1} \in Z(G)$.

On a montré que $Z(G)$ est un sous-groupe de G.

2) Notons $\mathcal{G}$ l'ensemble des matrices de la forme $\begin{pmatrix}1 & x & z\\ 0 & 1 & y\\ 0 & 0 & 1\end{pmatrix}$ avec x, y et $z \in \mathbb{R}$.

- $\mathcal{G}$ contient l'élément neutre I_3.

- Soit $M_1 = \begin{pmatrix} 1 & x_1 & z_1 \\ 0 & 1 & y_1 \\ 0 & 0 & 1 \end{pmatrix}$ et $M_2 = \begin{pmatrix} 2 & x_2 & z_2 \\ 0 & 1 & y_2 \\ 0 & 0 & 1 \end{pmatrix}$ deux élements de $\mathcal{G}$.

  On a $M_1M_2 = \begin{pmatrix} 1 & x_1 + x_2 & z_2 + x_1y_2 + z_1 \\ 0 & 1 & y_1 + y_2 \\ 0 & 0 & 1 \end{pmatrix} \in \mathcal{G}$

- Soit $M = \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$ un élément de $\mathcal{G}$.

  M est une matrice triangulaire dont les coefficients diagonaux sont non nuls donc M est inversible. On peut calculer son inverse à l'aide de la méthode de Gauss-Jordan ou à l'aide de la comatrice.

  On trouve $M^{-1} = \begin{pmatrix} 1 & -x & xy - z \\ 0 & 1 & -y \\ 0 & 0 & 1 \end{pmatrix}$. Ce qui prouve que $M^{-1} \in \mathcal{G}$.

Donc $\mathcal{G}$ est un sous-groupe du groupe linéaire donc c'est un groupe pour le produit matriciel.

Avec les notations précédentes, on a pour M_1 et M_2 dans $\mathcal{G}$:

$$M_1M_2 = M_2M_1 \quad \Longleftrightarrow \quad z_2 + x_1y_2 + z_1 = z_1 + x_2y_1 + z_2 \quad \Longleftrightarrow \quad x_1y_2 = x_2y_1$$

Si $M_1 \in Z(\mathcal{G})$, on a pour tous $x_2, y_2 \in \mathbb{R}$, $x_1y_2 = x_2y_1$.

En utilisant $(x_2, y_2) = (0, 1)$, on obtient $x_1 = 0$. De même avec $(x_2, y_2) = (1, 0)$, on obtient $y_1 = 0$.

Réciproquement si $M_1 = \begin{pmatrix} 1 & 0 & z_1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, on aura pour tout $M_2 \in \mathcal{G}$, $M_1M_2 = M_2M_1$.

Le centre du groupe $\mathcal{G}$ est l'ensemble des matrices de la forme $\begin{pmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ avec $z \in \mathbb{R}$.

Exercice 7

1) - Pour tout réel t, on a $t - \lfloor t \rfloor \in I$ donc $\star$ est une loi interne dans I.
   - L'addition étant commutative, la loi $\star$ est clairement commutative.
   - Montrons que $\star$ est associative :

     Soit x, y et $z \in I$. On a

$$\begin{aligned}
(x \star y) \star z &= (x \star y) + z - \lfloor (x \star y) + z \rfloor && \text{par définition de } \star \\
&= (x + y) - \lfloor x + y \rfloor + z - \big\lfloor (x + y) - \lfloor x + y \rfloor + z \big\rfloor && (*) \\
&= (x + y) - \lfloor x + y \rfloor + z - \lfloor (x + y) + z \rfloor + \lfloor x + y \rfloor && \text{calculs dans } (\mathbb{R}, +) \\
&= (x + y) + z - \lfloor (x + y) + z \rfloor && \text{associativité de } + \\
&= x + (y + z) - \lfloor x + (y + z) \rfloor && (**) \\
&= x \star (y \star z).
\end{aligned}$$

(*) d'une part $(x+y) - \lfloor x+y \rfloor + z = (x+y) + z - \lfloor x+y \rfloor$, d'autre part $n = \lfloor x+y \rfloor \in \mathbb{Z}$ et $\lfloor t-n \rfloor = \lfloor t \rfloor - n$ si $n \in \mathbb{Z}$.
(**) par des calculs semblables aux précédents.

- Pour tout $x \in I$, $\lfloor x \rfloor = 0$ donc $0 \star x = x \star 0 = x + 0 - \lfloor x+0 \rfloor = x$.
  Donc 0 est neutre pour $\star$.
- Pour tout $x \in I$, $(-x) \star x = x \star (-x) = x - x - \lfloor 0 \rfloor = 0$.
  Donc tout élément de I admet un symétrique pour $\star$.

On a montré que $(I, \star)$ est un groupe abélien.

2) Pour $x \in I$, $x \star x = 2x - \lfloor 2x \rfloor$ et $2x \in [0, 2[$ donc $\lfloor 2x \rfloor = 0$ ou 1.
Or $2x = \lfloor 2x \rfloor \iff 2x \in \mathbb{Z}$. Donc $x \star x = 0 \iff (2x = 0 \text{ ou } 2x = 1)$.
Donc $x \star x = 0$ a deux solutions $x = 0$ et $x = 1/2$.
Parmi ces solutions, seul $1/2$ est d'ordre 2.

3) Pour $n \in \mathbb{N}$ et $x \in I$, on note $x^{[n]}$ l'itéré de x d'ordre n pour la loi $\star$.
Soit $x \in I$. Pour $n \in \mathbb{N}$, on note $\mathcal{P}_n$: « $x^{[n]} = nx - \lfloor nx \rfloor$ ».
Par définition, 0 étant le neutre pour $\star$, $x^{[0]} = 0$. Donc $\mathcal{P}_0$ est vraie.
Soit $n \in \mathbb{N}$. On suppose $\mathcal{P}_n$ vraie.

$$\begin{aligned}
x^{n+1} &= x^{[n]} \star x \\
&= x^{[n]} + x - \lfloor x^{[n]} + x \rfloor && \text{par définition de } \star \\
&= nx - \lfloor nx \rfloor + x - \big\lfloor nx - \lfloor nx \rfloor + x \big\rfloor && \text{d'après } \mathcal{P}_n \\
&= nx + x - \lfloor nx \rfloor - \lfloor nx + x \rfloor + \lfloor nx \rfloor && \lfloor nx \rfloor \in \mathbb{Z} \\
&= (n+1)x - \lfloor nx \rfloor - \lfloor (n+1)x \rfloor.
\end{aligned}$$

Donc $\mathcal{P}_{n+1}$ est vraie.
On a montré par récurrence que pour tout $n \in \mathbb{N}$, $x^{[n]} = nx - \lfloor nx \rfloor$.
Comme $x \in I$, $nx \in [0, n[$ et on obtient :

$$x^{[n]} = 0 \iff \exists k \in \llbracket 0, n-1 \rrbracket, nx = k.$$

Donc $x^{[n]} = 0$ admet n solutions qui sont $x_k = \frac{k}{n}$ pour $k \in \llbracket 0, n_1 \rrbracket$.
Parmi ces solutions cherchons les éléments d'ordre exactement n :
On peut exclure $k = 0$ car 0 est d'ordre 1.
Soit $k \in \llbracket 1, n-1 \rrbracket$.
Pour $p \in \llbracket 1, n \rrbracket$, on a

$$x_k^{[p]} = 0 \iff px_k = \lfloor px_k \rfloor \iff p\frac{k}{n} \in \mathbb{Z} \iff n | pk.$$

- Si $k \wedge n = 1$. La condition n divise pk entraîne que n divise p donc $p = n$. Donc x_k est d'ordre exactement n.
- Sinon, notons $a = k \wedge n$. Il existe des entiers k' et n' tels que $k = ak'$ et $n = an'$.
  On remarque que $n' \in \llbracket 1, n-1 \rrbracket$ et que $n'k = n'ak' = nk'$ donc $x_k^{[n']} = 0$.
  Donc x_k n'est pas d'ordre n.
  Les éléments d'ordre n sont les $x_k = \frac{k}{n}$ avec $k \in \llbracket 1, n-1 \rrbracket$ premier avec n.

Exercices axés sur le raisonnement

Exercice 8

Soit H_1 et H_2 deux sous-groupes du groupe G (noté multiplicativement).

$\Longrightarrow$ Si $H_1 \subset H_2$ alors $H_1 \cup H_2 = H_2$ qui est un sous-groupe. Il en va de même si $H_2 \subset H_1$.

$\Longleftarrow$ On suppose que $H_1 \cup H_2$ est un sous-groupe.
On raisonne par l'absurde en supposant que H_1 n'est pas inclus dans H_2 et que H_2 n'est pas inclus dans H_1.
Il existe donc $x_1 \in H_1 \setminus H_2$ et $x_2 \in H_2 \setminus H_1$.
x_1 et x_2 étant deux éléments du groupe $H_1 \cup H_2$, $x_1x_2 \in H_1 \cup H_2$. Par symétrie des rôles, on peut supposer que $x_1x_2 \in H_1$. Écrivant alors $x_2 = x_1^{-1}(x_1x_2)$, on obtient $x_2 \in H_1$ (produit de deux éléments du groupe H_1) ce qui amène une contradiction puisque $x_2 \in H_2 \setminus H_1$.
On a donc prouvé que H_1 est inclus dans H_2 ou H_2 est inclus dans H_1.

Exercice 9

On note $f : G \to G, x \mapsto x^{-1}$.
On sait que pour tout $x \in G$, $\left(x^{-1}\right)^{-1} = x$ ce qui s'écrit $f \circ f(x) = x$ donc f est une involution de G et en particulier est bijective de G dans lui-même.
Soit x et y dans G. On a les équivalences suivantes :

$$\begin{aligned} f(x*y) = f(x)*f(y) &\iff (x*y)^{-1} = x^{-1}*y^{-1} \\ &\iff x*y = \left(x^{-1}*y^{-1}\right)^{-1} \\ &\iff x*y = y*x \end{aligned}$$

$a = b \iff a^{-1} = b^{-1}$

$(a*b)^{-1} = b^{-1}*a^{-1}$

Donc

$$\forall x, y \in G, f(x*y) = f(x)*f(y) \quad \iff \quad \forall x, y \in G, x*y = y*x.$$

Donc f est un morphisme si, et seulement si, $*$ est commutative.
On a montré que f est un isomorphisme du groupe $(G,*)$ dans lui-même si, et seulement si, le groupe $(G,*)$ est commutatif.

Exercice 10

1) Si $M \in \mathcal{M}_2(\mathbb{Z})$ alors $\det(M)$ est un entier.
Si M est inversible, on a $M^{-1}M = I_2$ donc $\det(M^{-1})\det(M) = 1$.
Donc si M^{-1} est aussi à coefficients entiers, alors $\det(M)$ est un entier inversible dans $\mathbb{Z}$ donc $\det(M) = \pm 1$.

2) On sait que $\left(\mathrm{GL}_2(\mathbb{R}), \times\right)$ est un groupe.
- $\mathrm{GL}_2(\mathbb{Z})$ est inclus dans $\mathrm{GL}_2(\mathbb{R})$.
- $\mathrm{GL}_2(\mathbb{Z})$ est non vide (il contient la matrice I_2).
- $\mathrm{GL}_2(\mathbb{Z})$ est stable par multiplication (car le produit de deux matrices de déterminants ± 1 est également de déterminant ± 1 et le produit de deux matrices à coefficients dans $\mathbb{Z}$ est aussi à coefficients dans $\mathbb{Z}$).

CORRECTIONS

- Soit $M \in \mathrm{GL}_2(\mathbb{Z})$.
  On sait que $\det(M) = \pm 1$ donc M est inversible et $\det(M^{-1}) = \frac{1}{\det(M)} = \pm 1$.
  De plus il existe $a, b, c, d \in \mathbb{Z}$ tels que $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
  On a alors $M^{-1} = \frac{1}{\det(M)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \pm \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$.

Par caractérisation des sous-groupes, $\mathrm{GL}_2(\mathbb{Z})$ est un sous-groupe de $\big(\mathrm{GL}_2(\mathbb{R}), \times\big)$.
Donc $\mathrm{GL}_2(\mathbb{Z})$ muni de $\times$ est un groupe.

3) Le calcul matriciel donne $A^2 = -I_2$, $A^3 = -A$ et $A^4 = I_2$. A est donc d'ordre 4.
De même, $B^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$ et $B^3 = I_2$. B est donc d'ordre 3.
On a $C = AB = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$. Afin de calculer les puissances successives de C, on écrit $C = -I_2 + N$ en posant $N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.
Cette matrice N commute avec I_2 et vérifie $N^2 = 0$. Donc la formule du binôme donne

$$C^n = (-1)^n I_2 + (-1)^{n-1} nN + 0 = (-1)^n \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}.$$

Remarque
On pouvait calculer les puissances successives de C par récurrence.

Donc $C^n \neq I_2$ pour $n \geqslant 1$. C est donc d'ordre infini.
On peut en conclure qu'il est possible que le produit de deux éléments d'ordre fini soit d'ordre infini.

Remarque
On peut aussi en déduire que A et B ne commutent pas. En effet si $AB = BA$, on aurait $(AB)^{12} = A^{12}B^{12} = I_2$. Néanmoins il suffit plus simplement de calculer BA pour constater $AB \neq BA$.

Exercice 11

1) Par définition de la loi produit, on a $(h, k)^n = (h^n, k^n)$ pour tout $n \in \mathbb{N}$. On sait que l'élément neutre de $H \times K$ est le couple $(1_H, 1_k)$.

$$\begin{aligned} (h,k)^n = 1_{H\times K} &\iff (h^n, k^n) = (1_H, 1_k) \\ &\iff \begin{cases} h^n = 1_H \\ k^n = 1_K \end{cases} \\ &\iff \begin{cases} p \mid n \\ q \mid n \end{cases} \\ &\iff \mathrm{ppcm}(p,q) \mid n \end{aligned}$$

h est d'ordre p,
k est d'ordre q

Donc le plus petit entier naturel $n \geqslant 1$ tel que $(h,k)^n = 1_{H\times K}$ est $\operatorname{ppcm}(p,q)$.
L'ordre de (h,k) est $\operatorname{ppcm}(p,q)$.

2) On note h un générateur de H et k un générateur de K.
Donc h est d'ordre $p = \operatorname{card}(H)$ et k est d'ordre $q = \operatorname{card}(K)$.
On sait que $H \times K$ est de cardinal pq. Il est donc cyclique si, et seulement si, il possède un élément d'ordre pq.

Si p et q sont premiers entre eux. Alors $\operatorname{ppcm}(p,q) = pq$ et, d'après la question précédente (h,k) est d'ordre pq : $H \times K$ est donc cyclique.

Si p et q ne sont pas premiers entre eux. Notons $r = \operatorname{ppcm}(p,q)$. On a $r < pq$.
Soit $x \in H \times K$. Il existe $a \in K$ et $b \in K$ tels que $x = (a,b)$. On a $x^r = (a,b)^r = (a^r, b^r)$.
On a $a^r = 1_H$ car p divise r et $b^r = 1_K$ car q divise r. Donc $x^r = 1_{H\times K}$. L'ordre de r est donc strictement inférieur à pq (car il divise r).
$H \times K$ n'est pas cyclique.

On a montré que $H \times K$ est cyclique si, et seulement si, p et q sont premiers entre eux.

Exercice 12

On note p le cardinal de G.

1) Soit $z \in G$. On sait que $z^p = 1$. En particulier $|z| = 1$.
Donc $G \subset \{z \in \mathbb{C} \mid |z| = 1\}$.

2) On a vu que $G \subset \mathbb{U}_p$ où $p = \operatorname{card}(G)$.
Puisque $\mathbb{U}_p$ est aussi de cardinal p, on a $G = \mathbb{U}_p$.

Exercice 13

1) $\mathbb{U}_\infty = \bigcup\limits_{n\in\mathbb{N}^*} \mathbb{U}_n$. En particulier

$$\left\{\exp\left(\frac{2i\pi}{n}\right), n \in \mathbb{N}^*\right\} \subset \mathbb{U}_\infty.$$

Or $\left(\frac{2\pi}{n}\right)_{n\in\mathbb{N}^*}$ est une suite de nombres 2 à 2 distincts de $]0, 2\pi]$, donc $\left(\exp\left(\frac{2i\pi}{n}\right)\right)_{n\in\mathbb{N}^*}$ est une suite de nombres complexes 2 à 2 distincts. Donc $\mathbb{U}_\infty$ est infini.

2) On sait que $(\mathbb{C}^*, \times)$ est un groupe.
- $\mathbb{U}_\infty$ est inclus dans $\mathbb{C}^*$.
- $\mathbb{U}_\infty$ est non vide (il est même infini).
- Soit z_1 et $z_2 \in \mathbb{U}_\infty$.
  Notons n_1 et n_2 deux entiers naturels non nuls tels que $z_1^{n_1} = 1$ et $z_2^{n_2} = 1$.
  On a $(z_1z_2)^{n_1n_2} = \left(z_1^{n_1}\right)^{n_2}\left(z_2^{n_2}\right)^{n_1} = 1$. Donc $z_1z_2 \in \mathbb{U}_\infty$ (car $n_1n_2 \in \mathbb{N}^*$).
  $\mathbb{U}_\infty$ est stable par multiplication.
- Soit $z \in \mathbb{U}_\infty$ et $n \in \mathbb{N}^*$ tel que $z^n = 1$. On a alors $\left(z^{-1}\right)^n = (z^n)^{-1} = 1$. Donc $z^{-1} \in \mathbb{U}_\infty$.

Par caractérisation des sous-groupes, $\mathbb{U}_\infty$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

CORRECTIONS

3) On raisonne par l'absurde, on suppose qu'il existe une partie A finie et engendrant le sous-groupe $\mathbb{U}_\infty$.

En notant N le PPCM des ordres des éléments de A, on a pour tout $a \in A, a^N = 1$.

Comme la multiplication de $\mathbb{C}^*$ est commutative et que tout élément de $\mathbb{U}_\infty$ est un produit fini d'éléments de A, on aurait pour tout $z \in \mathbb{U}_\infty, z^N = 1$.

Or $\omega = \exp\left(\frac{\mathrm{i}\pi}{N}\right)$ vérifie $\omega^N = \exp(\mathrm{i}\pi) = -1$ et $\omega \in \mathbb{U}_\infty$ car $\omega^{2N} = 1$.

On a ainsi au moins un élément de $\mathbb{U}_\infty$ qui ne vérifie pas $z^N = 1$ ce qui constitue une contradiction.

On a prouvé que $\mathbb{U}_\infty$ n'est pas engendré par une partie finie.

Exercice 14

1) L'image de f est l'ensemble noté HK par l'énoncé.

Soit $(h, k) \in H \times K$. On va montrer que pour tout $(h_1, k_1) \in H \times K$:

$$f(h_1, k_1) = hk \iff \exists x \in H \cap K, h_1 = hx \text{ et } k_1 = x^{-1}k.$$

$\Longrightarrow$ Soit $x \in H \cap K$. On pose $h_1 = hx$ et $k_1 = x^{-1}k$.
On a h et x appartiennent au sous-groupe H donc $h_1 \in H$.
De même $k_1 \in K$ car k et x^{-1} appartiennent à ce sous-groupe.
Et on a $f(h_1, k_1) = hxx^{-1}k = hk$.

$\Longleftarrow$ Soit $(h_1, k_1) \in K \times K$ tel que $h_1k_1 = hk$.
En multipliant par h^{-1} à gauche et par k_1^{-1} à droite on a $h^{-1}h_1 = kk_1^{-1}$.
Notons $x = h^{-1}h_1$. x appartient au sous-groupe H. Or $x = kk_1^{-1}$ donc x appartient aussi au sous-groupe K.
Donc $x \in H \cap K$ et on a $hx = h_1$ et $k_1 = x^{-1}k$.

Enfin l'équivalence $(hx = hx' \iff x = x')$ montre qu'il y a autant de couples (h_1, k_1) tels que $f(h_1, k_1) = hk$ que d'éléments x dans $H \cap K$. Donc chaque élément de HK possède $\mathrm{Card}(H \cap K)$ antécédents par f.

2) Notons $\tilde{f} : H \times K \to HK, (h, k) \mapsto hk$.

Par construction $\tilde{f}$ est surjective. Tout élément de HK a exactement $n = \mathrm{Card}(H \cap K)$ antécédents par $\tilde{f}$. Ce qui permet de former une partition de $H \times K$ en $\mathrm{Card}(HK)$ parties toutes de cardinal n. Donc $n\,\mathrm{Card}(HK) = \mathrm{Card}(H \times K) = \mathrm{Card}(H)\mathrm{Card}(K)$.

On a donc

$$\mathrm{Card}(HK)\mathrm{Card}(H \cap K) = \mathrm{Card}(H)\mathrm{Card}(K)$$

Exercice 15

1) On sait que $a^{\text{card}(G)} = e$ et que $e \in H$ car H est un sous-groupe.
Donc l'ensemble $\{p \in \mathbb{N}^* \mid a^p \in H\}$ est non vide car il contient $\text{card}(G)$. Il est inclus dans $\mathbb{N}$ et possède donc un minimum n.

2) Comme $a^n \in H$, le sous-groupe $\langle a^n \rangle$ engendré par a^n est un sous-groupe de H.
Il s'agit de voir que tout élément de H est un itéré de a^n.
Soit $x \in H$. Donc $x \in G$ et puisque a engendre G, il existe $p \geqslant 1$ tel que $x = a^p$.
On effectue la division euclidienne de p par n : $p = qn + r$ avec $0 \leqslant r \leqslant n - 1$.
On a alors $x = a^p = a^{nq}a^r$. Donc $a^r = (a^{nq})^{-1}x$. Or $a^{np} = (a^n)^q \in H$ et x aussi donc $a^r \in H$ (car H est un sous-groupe). Par minimalité de n, on en déduit $r = 0$.
Donc $x = a^p = (a^n)^q \in \langle a^n \rangle$.
Finalement, on a prouvé que $H = \langle a^n \rangle$ donc que H est cyclique.

Exercice 16

1) $A \cup B$ est une partie de G de cardinal $\text{Card}(A) + \text{Card}(B) - \text{Card}(A \cap B) = 2n - 1$.
Donc il existe $c \in G$ tel que $A \cup B \cup \{c\} = G$.

2) Soit $a \in A \setminus \{e\}, b \in B \setminus \{e\}$.
On raisonne par l'absurde. On suppose $a * b \neq c$. On a alors $a * b \in A \cup B$.
Les rôles de A et B étant symétriques, on peut supposer que $a * b \in A$ pour la démonstration . On a alors $b = a^{-1} * (a * b)$ qui appartiendrait au sous-groupe A. Donc $b \in A \cap B$.
On aurait donc $b \in \{e\}$ ce qui est impossible car $b \neq e$.
On a montré par l'absurde que $a * b = c$.
Donc
$$\forall a \in A \setminus \{e\}, \forall b \in B \setminus \{e\}, \quad a * b = c$$
Soit a et a' deux éléments de $A \setminus \{e\}$.
En utilisant un élément $b \in B \setminus \{e\}$, on a $a * b = c$ et $a' * b = c$. Donc $a * b = a' * b$ et, en multipliant par b^{-1} à droite, on obtient $a = a'$.
Donc $A \setminus \{e\}$ ne contient qu'un seul élément. D'où $n = 2$.

Remarque
On peut obtenir un exemple de cette situation en prenant $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et les sous-groupes $A = \mathbb{Z}/2\mathbb{Z} \times \{0\}$ et $B = \{0\} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 17

1) En notant multiplicativement les lois, on a $x^p = e$ donc $f\left(x^p\right) = f(e)$. Or f étant un morphisme $f(e) = e'$ et $f(x)^p = f\left(x^p\right)$ (voir exercice 1). Donc $f(x)^p = e'$. On peut donc affirmer que l'ordre de $f(x)$ dans G' est un diviseur de p.

Remarque
En version additive, on écrit $px = 0_G$ donc $pf(x) = f(px) = f(0_G) = 0_{G'}$.

CORRECTIONS

2) Soit f un morphisme de groupe de $\mathbb{Z}/7\mathbb{Z}$ dans $\mathbb{Z}/15\mathbb{Z}$.

Pour tout $x \in \mathbb{Z}/7\mathbb{Z}$, l'ordre de $f(x)$ divise 7 d'après la question précédente. Or $f(x)$ appartenant à $\mathbb{Z}/15\mathbb{Z}$, son ordre divise 15. Un entier naturel qui divise 7 et 15 est égal à 1. Donc $f(x)$ est ordre 1. Seul l'élément neutre étant d'ordre 1, on a $f(x) = 0$.

Donc f est l'application nulle.

Réciproquement, l'application nulle est un morphisme de groupe de $\mathbb{Z}/7\mathbb{Z}$ dans $\mathbb{Z}/15\mathbb{Z}$.

3) Soit f un morphisme de groupe de $\mathbb{Z}/4\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$.

On sait que $\mathbb{Z}/4\mathbb{Z}$ est un groupe cyclique engendré par la classe de 1 modulo 4 que nous noterons $\mathrm{cl}_4(1)$.

L'ordre de $f\big(\mathrm{cl}_4(1)\big)$ divise 4 d'après la première question et appartenant à $\mathbb{Z}/6\mathbb{Z}$, son ordre divise également 6. Donc son ordre divise 2.

Si son ordre est 1, on obtient $f\big(\mathrm{cl}_4(1)\big) = 0$ et f est l'application nulle.

Si son ordre est 2. Alors $f\big(\mathrm{cl}_4(1)\big) = \mathrm{cl}_6(3)$ (seul élément de $\mathbb{Z}/6\mathbb{Z}$ dont l'ordre est 2).

On obtient ensuite pour tout $n \in \mathbb{Z}$, $f\big(n\mathrm{cl}_4(1)\big) = n\mathrm{cl}_6(3)$.

Ainsi f est l'application qui, pour tout $n \in \mathbb{Z}$, associe à $\mathrm{cl}_4(n)$ l'élément $\mathrm{cl}_6(3n)$.

Cette application est bien définie car si $n' \in \mathrm{cl}_4(n)$ alors il existe $k \in \mathbb{Z}$ tel que $n' = n+4k$. Donc $3n' = 3n + 12k$ et $\mathrm{cl}_6(3n') = \mathrm{cl}_6(3n)$.

Réciproquement l'application nulle et l'application f précédente sont bien des morphismes de groupes (additifs) de $\mathbb{Z}/4\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$.

Exercice 18

On veut montrer qu'il existe $d \in \mathbb{N}^*$ tel que $N = 1 + 10 + 10^2 + \cdots + 10^{d-1}$ soit un multiple de 23.

Or $\sum_{k=0}^{d-1} 10^k = \frac{10^d-1}{10-1} = \frac{10^d-1}{9}$. Il s'agit de prouver l'existence d'un d tel que $10^d - 1$ soit un multiple de $23 \times 9 = 207$.

Or 10 est premier avec 207 donc la classe de 10 modulo 207 est dans le groupe des inversibles de $\mathbb{Z}/207\mathbb{Z}$. Cette classe est donc d'ordre fini dans ce groupe. Il existe $d \in \mathbb{N}^*$ tel que $10^d \equiv 1[207]$.

Il existe donc $q \in \mathbb{N}$ tel que $10^d - 1 = 23 \cdot 9q$. Donc $\frac{10^d-1}{9}$ est un multiple de 23 et il s'écrit uniquement avec des 1 en base dix.

Remarque

On peut être plus précis. Comme 9 et 23 sont premiers entre eux et que 9 divise $10^d - 1$, il suffit de chercher d tel que $10^d - 1$ soit un multiple de 23. On peut utiliser la démarche précédente dans $(\mathbb{Z}/23\mathbb{Z})^*$. L'ordre de la classe de 10 modulo 23 est un diviseur du cardinal du groupe des inversibles de $\mathbb{Z}/23\mathbb{Z}$ donc de $\varphi(23) = 22$ (car 23 est premier). En conclusion le nombre

$$N = \frac{10^{22} - 1}{9} = 1\,111\,111\,111\,111\,111\,111\,111$$

est un multiple de 23.

Exercices avec questions ouvertes

Exercice 19

1) Si G est fini, il y a un nombre fini de parties de G. En particulier G a un nombre fini de sous-groupes.

2) Réciproquement, supposons que G ait un nombre fini de sous-groupes.

• ***Montrons que tout élément de G est d'ordre fini.***

On raisonne par l'absurde. On suppose qu'il existe $x \in G$ d'ordre infini. Notons $H_k = \langle x^k \rangle$ pour $k \in \mathbb{N}$.

Soit k et $k' \in \mathbb{N}$. Montrons que si $H_k = H_{k'}$, alors $k = k'$.

Si $H_k = H_{k'}$, alors $x^k \in H_{k'}$. Donc il existe $p \in \mathbb{Z}$ tel que $x^k = x^{pk'}$. Or x étant d'ordre infini, cela entraînerait que $k = pk'$. Donc k' divise k. Les rôles étant symétriques, on obtient aussi k divise k'. Finalement $k = k'$.

Donc les sous-groupes H_k pour $k \in \mathbb{N}$ sont deux à deux distincts.

On aurait une infinité de sous-groupes distincts, ce qui est impossible.

On a montré par l'absurde que tout élément est d'ordre fini.

• ***Montrons que G est fini.***

En remarquant que $G = \bigcup_{x \in G} \langle x \rangle$, on en déduit, puisqu'il existe un nombre fini de sous-groupes distincts, qu'il existe $x_1, x_2, \dots, x_n$ tels que

$$G = \bigcup_{k=1}^{n} \langle x_k \rangle$$

Or les sous-groupes $\langle x_k \rangle$ sont finis donc $G = \bigcup_{k=1}^{n} \langle x_k \rangle$ l'est aussi.

Exercice 20

Soit $\varphi : \mathbb{Q} \to \mathbb{Z}$ un morphisme de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.
On a en particulier

$$\forall q \in \mathbb{N}^*, \quad \varphi(1) = \varphi\left(q\frac{1}{q}\right) = q\varphi\left(\frac{1}{q}\right)$$

Comme φ est à valeurs dans $\mathbb{Z}$, $\varphi(1)$ est ainsi un entier divisible par tout $q \in \mathbb{N}^*$. On a donc $\varphi(1) = 0$. Puis pour tout $q \in \mathbb{N}^*$, $\varphi(1/q) = 0$ puisque $q\varphi(1/q) = \varphi(1) = 0$.
Finalement

$$\forall p \in \mathbb{Z}, \forall q \in \mathbb{N}^*, \quad \varphi\left(\frac{p}{q}\right) = p\varphi\left(\frac{1}{q}\right) = 0.$$

φ est donc l'application nulle.
Réciproquement l'application nulle est un morphisme de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.

CORRECTIONS

Exercice 21

Notons d l'ordre de σ. Montrons que si d est impair alors $\varepsilon(\sigma) = 1$.
On sait que $\sigma^d = \mathrm{Id}_{[\![1,n]\!]}$ et que la signature est un morphisme de groupes donc

$$\varepsilon(\sigma)^d = \varepsilon\left(\sigma^d\right) = \varepsilon\left(\mathrm{Id}_{[\![1,n]\!]}\right) = 1$$

Comme d est impair, $\varepsilon(\sigma) = -1$ est impossible. Donc $\varepsilon(\sigma) = 1$.

En revanche, il n'y a pas de résultat général lorsque d est pair.
Par exemple, une transposition est d'ordre 2 et est de signature -1 alors que le produit $\langle 1, 2\rangle \circ \langle 3, 4\rangle$ est aussi d'ordre 2 et est de signature 1.

Exercice 22

Soit $f : \mathbb{R} \to \mathbb{R}$ un morphisme de groupes continu sur $\mathbb{R}$.
Par une démonstration semblable à celle de l'exercice 2, on a

$$\forall r \in \mathbb{Q}, \quad f(r) = rf(1)$$

Pour $x \in \mathbb{R}$, on sait qu'il existe une suite $(r_n)_{n\in\mathbb{N}}$ de rationnels convergeant vers x. Par continuité de f on a $f(r_n) \xrightarrow[n\to\infty]{} f(x)$. Or $f(r_n) = r_n f(1) \xrightarrow[n\to\infty]{} xf(1)$.
Par unicité de la limite, on obtient $f(x) = xf(1)$.
Donc f est linéaire.
Réciproquement pour $a \in \mathbb{R}$, l'application $x \mapsto ax$ est continue sur $\mathbb{R}$ et est un morphisme de groupes.
Les morphismes de groupes continus de $(\mathbb{R}, +)$ dans lui-même sont les applications linéaires de $\mathbb{R}$ dans $\mathbb{R}$.

Anneaux 2

Exercices axés sur le calcul

Exercice 1

Soit p un nombre premier. Dans $\mathbb{Z}/p\mathbb{Z}$, calculer les sommes $s_1 = \sum_{k=1}^{p} \overline{k}$ et $s_2 = \sum_{k=1}^{p} \overline{k}^2$

Exercice 2

Résoudre dans $\mathbb{Z}$, le système $(\mathcal{H})\begin{cases} x \equiv 0\ [10] \\ x \equiv 0\ [13] \end{cases}$ puis le système $(S)\begin{cases} x \equiv 2\ [10] \\ x \equiv 5\ [13] \end{cases}$.

Exercice 3

Déterminer le groupe des inversibles de l'anneau $\mathbb{Z}/8\mathbb{Z}$. Ce groupe est-il cyclique ?

Exercice 4

Soit $A = \left\{ \dfrac{m}{2^n} \;\middle|\; m \in \mathbb{Z} \text{ et } n \in \mathbb{N} \right\}$.

1) Montrer que A est un sous-anneau de $(\mathbb{Q}, +, \times)$.
2) Quels en sont les éléments inversibles ?

Exercice 5

Soit E l'ensemble des matrices de la forme $\begin{pmatrix} a & 2b \\ -b & a \end{pmatrix}$ avec a et b réels.

1) Montrer que E est un sous-espace vectoriel de $\mathcal{M}_2(\mathbb{R})$ et donner sa dimension.
2) Montrer que E est un sous-anneau de $\mathcal{M}_2(\mathbb{R})$ puis que E est un corps.
3) Résoudre dans E, l'équation $X^2 = I_2$.

D'après CCINP

Exercice 6 ⋆ *Symbole de Pochhammer*

Soit $(A, +, \times)$ un anneau commutatif. Pour $x \in A$ et $n \in \mathbb{N}$, on définit $x^{(n)}$ par :

$$x^{(0)} = 1_A, \qquad x^{(n)} = x(x-1)\cdots(x-n+1).$$

Montrer que pour tous x et $y \in A$ et tout $n \in \mathbb{N}$, on a :

$$(x+y)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} x^{(k)} y^{(n-k)}.$$

Exercices axés sur le raisonnement

Exercice 7 *Radical d'un idéal*

Soit $(A, +, \times)$ un anneau commutatif, I un idéal de A.
On note $R(I)$ l'ensemble des éléments x de A tel qu'il existe n dans $\mathbb{N}^*$ tel que $x^n \in I$.

1) Montrer que $R(I)$ est un idéal de A contenant I.
2) On considère l'ensemble $E = \{n \in \mathbb{N}^* \mid R(n\mathbb{Z}) = n\mathbb{Z}\}$.
   Montrer que E est l'ensemble des entiers naturels qui ne sont pas divisibles par le carré d'un nombre premier.

D'après Mines-Télécom

Exercice 8 *Classique*

Soit p un nombre premier supérieur à 3. On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. On rappelle que $\mathbb{F}_p$ est un corps.

1) Montrer que $f : x \mapsto x^2$ est un morphisme de groupes de $(\mathbb{F}_p^*, \times)$ dans lui-même.
2) Montrer que $\mathrm{Ker}(f) = \left\{\overline{1}, -\overline{1}\right\}$.
3) Montrer que pour tout $x \in \mathbb{F}_p^*$, $x^{\frac{p-1}{2}} = \overline{1}$ ou $-\overline{1}$.
4) Montrer qu'il y a $\frac{p-1}{2}$ carrés dans $\mathbb{F}_p^*$.

D'après CCINP

Exercice 9 *Un anneau qui n'est pas un sous-anneau*

On considère le sous-espace vetoriel E engendré par les deux matrices réelles suivantes

$$A = \begin{pmatrix} -1 & 0 & 1 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix} \text{ et } B = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & 0 & -1 \end{pmatrix}.$$

1) Montrer que $(E, +, \times)$ (où $\times$ est la multiplication matricielle usuelle) est un anneau mais que ce n'est pas un sous-anneau de $\mathcal{M}_3(\mathbb{R})$.
2) La matrice A est-elle inversible dans $\mathcal{M}_3(\mathbb{R})$? Admet-elle un inverse dans l'anneau E c'est-à-dire une matrice $M \in E$ telle que $MA = AM = 1_E$ où 1_E désigne l'élément neutre pour $\times$ dans l'anneau E ?

Exercice 10 *Anneau de Boole*

Soit $(A, +, \times)$ un anneau. On suppose que

$$\forall x \in A, \quad x^2 = x. \tag{$\star$}$$

1) Montrer que pour tout $x \in A$, $2x = 0$.
2) Montrer que A est commutatif.
   Indication : On pourra envisager $(x + y)^2$.
3) Quels sont les éléments inversibles de A ?

Exercice 11

Soit a et n des entiers naturels strictement supérieurs à 1. On note $N = a^n - 1$.

1) Montrer que $\overline{a}$ est inversible dans l'anneau $\mathbb{Z}/N\mathbb{Z}$ et déterminer l'ordre de a dans le groupe des inversibles $U(\mathbb{Z}/N\mathbb{Z})$.
2) En déduire que n divise $\varphi(N)$ (φ désigne l'indicatrice d'Euler).

Exercice 12

1) *Exemple*
   Soit $k \in \mathbb{N}^*$. Préciser les diviseurs de 0 de l'anneau $\mathbb{Z}/2^k\mathbb{Z}$.
2) On considère A un anneau commutatif fini. On suppose que A possède n diviseurs de zéro, avec $n > 1$.
   a) Soit a un diviseur de 0.
      Montrer que $f : A \to A, x \mapsto ax$ est un morphisme de groupes de $(A, +)$ dans lui-même et que tout élément $y \in \mathrm{Im}(f)$ admet exactement $\mathrm{card}\big(\mathrm{Ker}(f)\big)$ antécédents.
   b) En déduire que A a au plus $(n + 1)^2$ éléments.

D'après ENS

Exercices avec questions ouvertes

Exercice 13 Quels sont les morphismes d'anneaux de $(\mathbb{Z}, +, \times)$ dans lui-même ?

Exercice 14 *Classique*

Quels sont les morphismes d'anneaux de $(\mathbb{R}, +, \times)$ dans lui-même ?
Indication : On pourra montrer qu'un tel morphisme est croissant.

D'après Mines-Télécom

Exercice 15 ★★

Soit $(A, +, \times)$ un anneau.

1) Montrer que si la multiplication est commutative alors $f : A \to A, x \mapsto x^2$ est un morphisme multiplicatif c'est-à-dire qu'on a :

$$\forall x, y \in A, \quad (xy)^2 = x^2y^2. \tag{$\star$}$$

2) La réciproque est-elle vraie ?

Indication : On pourra commencer par utiliser $(\star)$ pour x et $1_A + y$.

Corrections

Exercices axés sur le calcul

Exercice 1

Notons $S_1 = \sum\limits_{k=1}^{p} k$ et $S_2 = \sum\limits_{k=1}^{p} k^2$. Ce sont des naturels et on a $s_1 = \overline{S_1}$ et $s_2 = \overline{S_2}$.

On sait que $S_1 = \sum\limits_{k=1}^{p} k = \frac{p(p+1)}{2}$. Donc 2 divise $p(p+1)$. Distinguons deux cas :

- Si $p = 2$, $S_1 = 3$ donc $S_1 \equiv 1\ [2]$. Donc $s_1 = \overline{1}$ dans $\mathbb{Z}/2\mathbb{Z}$.
- Sinon p est impair donc $\frac{p+1}{2} \in \mathbb{N}$. Donc S_1 est un multiple de p et $s_1 = \overline{0}$.

De même $S_2 = \sum\limits_{k=1}^{p} k^2 = \frac{p(p+1)(2p+1)}{6}$. Distinguons trois cas :

- Si $p = 2$, $S_2 = 5$ donc $S_2 \equiv 1\ [2]$. Donc $s_2 = \overline{1}$ dans $\mathbb{Z}/2\mathbb{Z}$.
- Si $p = 3$, $S_2 = 14$ donc $S_2 \equiv 2\ [3]$. Donc $s_2 = \overline{2}$ dans $\mathbb{Z}/3\mathbb{Z}$.
- Sinon p et 6 sont premiers entre eux donc 6 divise $(p+1)(2p+1)$. Donc S_2 est un multiple de p et $s_2 = \overline{0}$.

Exercice 2

On a $(x \equiv 0\,[13] \iff 13|x)$ et $(x \equiv 0\,[10] \iff 10|x)$. Puisque 10 et 13 sont premiers entre eux, on obtient :

$$\begin{cases} x \equiv 0 \ [10] \\ x \equiv 0 \ [13] \end{cases} \iff 130|x \iff \exists q \in \mathbb{Z}, x = 130q.$$

Soit x_0 une solution de (S). On a pour tout $x \in \mathbb{Z}$:

$$\begin{cases} x \equiv 2 \ [10] \\ x \equiv 5 \ [13] \end{cases} \iff \begin{cases} x - x_0 \equiv 0 \ [10] \\ x - x_0 \equiv 0 \ [13] \end{cases} \iff \exists q \in \mathbb{Z}, x = x_0 + 130q$$

Il reste à déterminer une solution [particulière] x_0.

Première méthode (méthode générale)

Soit $x \in \mathbb{Z}$.

$$\begin{cases} x \equiv 2 \ [10] \\ x \equiv 5 \ [13] \end{cases} \iff \exists k, k' \in \mathbb{Z}, \begin{cases} x = 2 + 10k \\ x = 5 + 13k' \end{cases}$$

$$\iff \exists k, k' \in \mathbb{Z}, \begin{cases} x = 2 + 10k \\ 10k - 13k' = 3 \end{cases}$$

Puisque 10 et 13 sont premiers entre eux, on sait qu'il existe des coefficients (dits de Bézout) u et v entiers tels que $10u + 13v = 1$.
En écrivant l'algorithme d'Euclide (ou en devinant) on constate que $10 \cdot 4 - 13 \cdot 3 = 1$. On a donc $10 \cdot 12 - 13 \cdot 9 = 3$. Donc $x_0 = 2 + 10 \cdot 12 = 122$ est une solution de (S).

Deuxième méthode (en utilisant les inverses de $\mathbb{Z}/13\mathbb{Z}$)

Soit $k \in \mathbb{Z}$ et $x = 2 + 10k$. On a ainsi $x \equiv 2$ [10]. Puis

$x \equiv 5 \ [13] \iff 10k \equiv 3 \ [13]$.

Or $4 \cdot 10 = 40 \equiv 1$ [13] donc l'inverse de $\overline{10}$ dans $\mathbb{Z}/13\mathbb{Z}$ est $\overline{4}$. Donc

$x \equiv 5 \ [13] \iff k \equiv 4 \cdot 3 \ [13]$.

On peut choisir $k = 12$ et on a ainsi une solution particulière $x_0 = 2 + 120 = 122$.

Remarque

On a préféré travailler dans $\mathbb{Z}/13\mathbb{Z}$ car c'est un corps mais on aurait pu travailler dans l'anneau $\mathbb{Z}/10\mathbb{Z}$ et déterminer l'inverse de la classe de 13 modulo 10 (c'est la classe de 7 car $7 \cdot 13 = 91 \equiv 1$ [10]).

Finalement :

$$\begin{cases} x \equiv 2 \ [10] \\ x \equiv 5 \ [13] \end{cases} \iff \exists q \in \mathbb{Z} \mid x = 122 + 130q.$$

Exercice 3

Parmi les entiers de 1 à 7, ceux qui sont premiers avec 8 sont 1, 3, 5 et 7. On a donc

$$U(\mathbb{Z}/8\mathbb{Z}) = \left\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\right\}.$$

$\overline{1}$ est d'ordre 1. On a $\overline{3}^2 = \overline{9} = \overline{1}$. Donc $\overline{3}$ est d'ordre 2. Il n'engendre pas le groupe $\big(U(\mathbb{Z}/8\mathbb{Z}), \cdot\big)$.
De même $\overline{5}^2 = \overline{25} = \overline{1}$ et $\overline{7}^2 = \overline{49} = \overline{1}$, les éléments $\overline{5}$ et $\overline{7}$ sont aussi d'ordre 2.
Aucun des quatres éléments de $U(\mathbb{Z}/8\mathbb{Z})$ n'engendre le groupe $\big(U(\mathbb{Z}/8\mathbb{Z}), \cdot\big)$. Ce groupe n'est donc pas cyclique.

Exercice 4

1) Il est immédiat que $\mathbb{Z} \subset \mathbb{Q}$.
Pour tout $m \in \mathbb{Z}, m = \frac{m}{2^0}$ donc $\mathbb{Z} \subset A$ et en particulier A contient 1.
Soit $a_1, a_2 \in A$. Pour $i \in \{1, 2\}$, on choisit $m_i \in \mathbb{Z}$ et $n_i \in \mathbb{N}$ tels que $a_i = \frac{m_i}{2^{n_i}}$. On a alors :
   - $-a_1 = \frac{-m_1}{2^{n_1}} \in A$;

- $a_1 + a_2 = \frac{m_1}{2^{n_1}} + \frac{m_2}{2^{n_2}} = \frac{2^{n_2}m_1 + 2^{n_1}m_2}{2^{n_1+n_2}}$ donc $a_1 + a_2 \in A$ (car $2^{n_2}m_1 + 2^{n_1}m_2 \in \mathbb{Z}$) ;
- $a_1 a_2 = \frac{m_1}{2^{n_1}} \cdot \frac{m_2}{2^{n_2}} = \frac{m_1 m_2}{2^{n_1+n_2}}$ donc $a_1 a_2 \in A$.

Donc A est un sous-anneau de $(\mathbb{Q}, +, \times)$.

2) Soit $r = \frac{m}{2^n}$ avec $m \in \mathbb{Z}^*$ et $n \in \mathbb{N}$ un élément inversible de l'anneau A.

Il existe $r' = \frac{m'}{2^{n'}}$ avec $m' \in \mathbb{Z}^*$ et $n' \in \mathbb{N}$ tels que $rr' = 1$. D'où $2^{n+n'} = mm'$.

Donc m est une puissance de 2 (seul nombre premier pouvant diviser $2^{n+n'}$).
Il existe $k \in \mathbb{N}$ tel que $m = \pm 2^k$. Et donc $r = \pm 2^{k-n}$.
Les éléments inversibles sont de la forme de la forme $\pm 2^a$ avec $a \in \mathbb{Z}$.

Réciproquement montrons que ces nombres sont inversibles dans A :

- Si $r = \pm 2^k$ avec $k \in \mathbb{N}$. On a $r \in \mathbb{Z}$ donc $r \in A$ et $r^{-1} = \pm\frac{1}{2^k} \in A$.
- Sinon $r = \pm\frac{1}{2^k}$ avec $k \in \mathbb{N}^*$. On a $r \in A$ et $r^{-1} = \pm 2^k \in A$.

On a montré :

$$U(A) = \{\pm 2^a, a \in \mathbb{Z}\}.$$

Exercice 5

1) Notons $J = \begin{pmatrix} 0 & 2 \\ -1 & 0 \end{pmatrix}$ ainsi $\begin{pmatrix} a & 2b \\ -b & a \end{pmatrix} = aI_2 + bJ$.

Donc $E = \mathrm{Vect}(I_2, J)$ et E est un espace vectoriel. La famille génératrice trouvée étant libre (J n'est pas colinéaire à I_2), E est de dimension 2.

2) Puisque E est un sous-espace vectoriel, E est un sous-groupe de $(\mathcal{M}_2(\mathbb{R}), +)$.

E contient le neutre I_2.

Soit $M = \begin{pmatrix} a & 2b \\ -b & a \end{pmatrix} \in E$ et $M' = \begin{pmatrix} a' & 2b' \\ -b' & a' \end{pmatrix} \in E$.

$$MM' = \begin{pmatrix} a & 2b \\ -b & a \end{pmatrix}\begin{pmatrix} a' & 2b' \\ -b' & a' \end{pmatrix} = \begin{pmatrix} aa' - 2bb' & 2(ab' + ba') \\ -(ba' + ab') & aa' - 2bb' \end{pmatrix} \in E$$

Donc E est un sous-anneau de $(\mathcal{M}_2(\mathbb{R}), +, \times)$.

Remarque

En utilisant la base trouvée et le développement

$$(aI_2 + bJ)(a'I_2 + b'J) = aa'I_2 + (ab' + b'a)J + bb'J^2$$

il suffisait, compte tenu de la stabilité par combinaison linéaire, de vérifier que la matrice $J^2 = \begin{pmatrix} -2 & 0 \\ 0 & -2 \end{pmatrix}$ appartient effectivement à E.

Le calcul précédent montre également que deux matrices de E commutent pour $\times$.

Soit $M = \begin{pmatrix} a & 2b \\ -b & a \end{pmatrix} \in E \setminus \{0\}$.

On a $(a,b) \neq (0,0)$ et $\det(M) = a^2 + 2b^2 > 0$ (a et b sont des réels et au moins un est non nul). Donc $\det(M) \neq 0$ ce qui prouve que M est inversible.

Et on a $M^{-1} = \frac{1}{\det(A)} \begin{pmatrix} a & -2b \\ b & a \end{pmatrix} \in E$ car $a' = \frac{a}{\det(A)}$ et $b' = -\frac{b}{\det(A)}$ sont des réels.

Donc $(E, +, \times)$ est un anneau commutatif et tout élément non nul est inversible : c'est un corps.

3) Avec $M = \begin{pmatrix} a & 2b \\ -b & a \end{pmatrix}$ on a $\begin{pmatrix} a & 2b \\ -b & a \end{pmatrix}^2 = \begin{pmatrix} a^2 - 2b^2 & 4ab \\ -2ab & a^2 - 2b^2 \end{pmatrix}$.

Donc : $M^2 = I_2 \iff \begin{cases} a^2 - 2b^2 & = 1 \\ 2ab & = 0 \end{cases} \iff \begin{cases} b & = 0 \\ a^2 & = 1 \end{cases}$ ou $\begin{cases} a & = 0 \\ b^2 & = -1/2 \end{cases}$.

Le second système n'a pas de solution avec $b \in \mathbb{R}$.

L'équation $X^2 = I_2$ a deux solutions dans E qui sont I_2 et $-I_2$

Exercice 6

Soit x et $y \in A$.

Pour $n \in \mathbb{N}$, on note $\mathcal{P}_n$ la proposition « $(x+y)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} x^{(k)} y^{(n-k)}$ ».

Pour $n = 0$, on a $(x+y)^{(0)} = 1_A$ et $\sum_{k=0}^{0} \binom{0}{k} x^{(k)} y^{(0-k)} = \binom{0}{0} x^{(0)} y^{(0)} = 1_A$ donc $\mathcal{P}_0$ est vraie.

Soit $n \in \mathbb{N}$. On suppose $\mathcal{P}_n$ vraie. On a alors :

$$\begin{aligned}
(x+y)^{(n+1)} &= (x+y)^{(n)}(x+y-n) \\
&\underset{\text{d'après } \mathcal{P}_n}{=} \left(\sum_{k=0}^{n} \binom{n}{k} x^{(k)} y^{(n-k)} \right)(x+y-n) \\
&\underset{\text{par distributivité}}{=} \sum_{k=0}^{n} \binom{n}{k} x^{(k)} y^{(n-k)} (x+y-n)
\end{aligned}$$

Puis on utilise $x + y - n = x - k + y - (n-k)$ et on transforme $(x+y)^{(n+1)}$ en $S_1 + S_2$ avec $S_1 = \sum_{k=0}^{n} \binom{n}{k} x^{(k)}(x-k) y^{(n-k)}$ et $S_2 = \sum_{k=0}^{n} \binom{n}{k} x^{(k)} y^{(n-k)} \big(y - (n-k)\big)$.

Puisque $x^{(k)}(x-k) = x^{(k+1)}$, on a :

$$\begin{aligned}
S_1 &= \sum_{k=0}^{n} \binom{n}{k} x^{(k+1)} y^{(n-k)} \\
&\underset{\text{par changement d'indice}}{=} \sum_{k=1}^{n+1} \binom{n}{k-1} x^{(k)} y^{(n-k)} \\
&\underset{\binom{n}{n} = 1}{=} 1 x^{(n+1)} y^{(0)} + \sum_{k=1}^{n} \binom{n}{k-1} x^{(k)} y^{(n-k)} \\
&\underset{y^{(0)} = 1_A}{=} x^{(n+1)} + \sum_{k=1}^{n} \binom{n}{k-1} x^{(k)} y^{(n-k)}
\end{aligned}$$

De même $y^{(n-k)}\big(y-(n-k)\big) = y^{(n-k+1)}$ et :

$$\begin{aligned} S_2 &= \sum_{k=0}^{n} \tbinom{n}{k} x^{(k)} y^{(n-k+1)} \\ &= 1x^{(0)}y^{(n+1)} + \sum_{k=0}^{n} \tbinom{n}{k} x^{(k)} y^{(n-k+1)} && \tbinom{0}{0} = 1 \\ &= y^{(n+1)} + \sum_{k=0}^{n} \tbinom{n}{k} x^{(k)} y^{(n-k+1)} && x^{(0)} = 1_A \end{aligned}$$

Donc

$$\begin{aligned} (x+y)^{(n+1)} &= S_1 + S_2 \\ &= x^{(n+1)} + y^{(n+1)} + \sum_{k=1}^{n} \left(\tbinom{n}{k-1} + \tbinom{n}{k}\right) x^{(k)} y^{(n-k+1)} && \text{formule de Pascal} \\ &= x^{(n+1)} + y^{(n+1)} + \sum_{k=1}^{n} \tbinom{n+1}{k} x^{(k)} y^{(n-k+1)} \\ &= \sum_{k=0}^{n+1} \tbinom{n+1}{k} x^{(k)} y^{(n-k+1)} \end{aligned}$$

Ce qui montre que $\mathcal{P}_{n+1}$ est vraie.

On a montré par récurrence que :

$$\forall n \in \mathbb{N}, \quad (x+y)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} x^{(k)} y^{(n-k)}.$$

Exercices axés sur le raisonnement

Exercice 7

1) Il est immédiat que $I \subset R(I)$ (si $x \in I$ on a $x^1 = x \in I$). En particulier $R(I)$ est non vide.
Soit $x, y \in R(I)$. Il existe $n, m \in \mathbb{N}^*$ tels que $x^n \in I$ et $y^m \in I$.
L'anneau étant commutatif, la formule du binôme donne :

$$(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k}$$

Pour $k \geqslant n$, $x^k y^{n+m-k} = x^{k-n} y^{n+m-k} \times x^n \in I$ car I est un idéal.
Pour $k \leqslant n$, on a de même $x^k y^{n+m-k} = x^k y^{n-k} \times y^m \in I$.
$(I, +)$ étant un groupe, on a $(x+y)^{n+m} \in I$ (par addition) et donc $x + y \in R(I)$.
Et $(-x)^n = (-1_A)^n x^n \in I$ donc $-x \in R(I)$.
On a montré que $R(I)$ est un sous-groupe de $(A, +)$.

Soit $x \in R(I)$ et $n \in \mathbb{N}^*$ tel que $x^n \in I$.
Pour tout $z \in A$, la loi étant commutative on a $(zx)^n = z^n x^n \in I$ et donc $zx \in R(I)$.
$R(I)$ est ainsi un idéal (et il contient I).

2) On travaille ici dans l'anneau $(\mathbb{Z}, +, \times)$ qui est bien commutatif. On sait aussi qu'il est principal, c'est-à-dire que les idéaux sont exactement les $n\mathbb{Z}$ avec $n \in \mathbb{N}$.
Pour tout entier n on a $n\mathbb{Z} \subset R(n\mathbb{Z})$ (question précédente). Il s'agit donc de trouver les n pour lesquels l'inclusion réciproque est vraie.

• Soit $n \in \mathbb{N}^*$ tel que $R(n\mathbb{Z}) = n\mathbb{Z}$.
Décomposons n en produit de facteurs premiers : $n = p_1^{a_1} \dots p_k^{a_k}$.
En notant $m = p_1 \cdot p_2 \dots p_k$. On a $m^{\max(a_1,\dots,a_k)}$ est multiple de n donc $m \in R(n\mathbb{Z})$.
Donc $m \in n\mathbb{Z}$ puisque $R(n\mathbb{Z}) = n\mathbb{Z}$.
L'entier $p_1 \cdot p_2 \dots p_k$ étant un multiple de $n = p_1^{a_1} \dots p_k^{a_k}$, tous les a_i sont égaux à 1.
• Réciproquement soit $n = p_1 \cdot p_2 \dots p_k$ (où les p_j sont des nombres premiers deux à deux distincts).
Montrons l'inclusion $R(n\mathbb{Z}) \subset n\mathbb{Z}$.
Soit $m \in R(n\mathbb{Z})$. Il existe $k \in \mathbb{N}^*$ tel que $m^k \in n\mathbb{Z}$. Chacun des nombres premiers p_j divisant n devant diviser m^k, on a p_j divise m^k donc divise m.
Donc $n = p_1 \cdot p_2 \dots p_k$ divise m c'est-à-dire $m \in n\mathbb{Z}$.

On a donc montré :
$R(n\mathbb{Z}) = n\mathbb{Z}$ si, et seulement si, n n'est pas divisible par le carré d'un nombre premier.

Exercice 8

1) On sait que $(\mathbb{F}_p^*, \times)$ est un groupe commutatif. Donc pour tout $x \in \mathbb{F}_p^*$, $x^2 \in \mathbb{F}_p^*$ et :

$$\forall x, y \in \mathbb{F}_p^*, \quad f(xy) = (xy)^2 = x^2y^2 = f(x)\,f(y)\,.$$

Donc $f : x \mapsto x^2$ est un morphisme de groupes de $(\mathbb{F}_p^*, \times)$ dans lui-même.

2) Soit $x \in \mathbb{F}_p^*$.

$$\begin{aligned} x \in \operatorname{Ker}(f) &\iff f(x) = \overline{1} && \text{par définition de } f \\ &\iff x^2 = \overline{1} && \text{calcul dans } (\mathbb{F}_p, +) \\ &\iff x^2 - \overline{1} = \overline{0} && \text{calcul dans l'anneau} \\ &\iff \left(x - \overline{1}\right)\left(x + \overline{1}\right) = \overline{0} && \mathbb{F}_p \text{ est un corps} \\ &\iff x - \overline{1} = \overline{0} \quad \text{ou} \quad x + \overline{1} = \overline{0} \end{aligned}$$

On a montré que $\operatorname{Ker}(f) = \left\{\overline{1}, -\overline{1}\right\}$.

3) Soit $x \in \mathbb{F}_p^*$. L'entier p étant impair, on a $\frac{p-1}{2} \in \mathbb{N}$ et l'élément $y = x^{\frac{p-1}{2}}$ est bien défini.
On a alors $y^2 = x^{p-1}$. Or $p - 1$ est le cardinal du groupe $\mathbb{F}_p^*$ donc $x^{p-1} = \overline{1}$ (car l'ordre de x divise $p - 1$).
Donc $y^2 = 1$. D'après la question précédente $y = \pm\overline{1}$ donc $x^{\frac{p-1}{2}} = \overline{1}$ ou $-\overline{1}$.

CORRECTIONS

4) Soit $C = \{a^2, a \in \mathbb{F}_p^*\}$ l'ensemble des carrés de $\mathbb{F}_p^*$ et $\hat{f} : \mathbb{F}_p^* \to C, x \mapsto x^2$.
Par construction $\hat{f}$ est surjective. Donc $\mathbb{F}_p^* = \bigcup_{c \in C} \hat{f}^{-1}(\{c\})$. Or tout élément de C a exactement deux antécédents distincts par $\tilde{f}$ car :

$$x^2 = a^2 \iff x^2 - a^2 = \overline{0} \iff (x - a = \overline{0} \text{ ou } x + a = \overline{0}).$$

Ainsi on peut former une partition de $\mathbb{F}_p^*$ en $\mathrm{Card}(C)$ parties du type $\{a, -a\}$ toutes de cardinal 2 (car $a \neq -a$). Donc $2\,\mathrm{Card}(C) = \mathrm{Card}(\mathbb{F}_p^*) = p - 1$.
Donc il y a $\frac{p-1}{2}$ carrés dans $\mathbb{F}_p^*$.

Exercice 9

1) On sait que E est un sous-espace vectoriel. En particulier $(E, +)$ est un groupe.
Pour a et b réels on a $aA + bB = \begin{pmatrix} -a-b & b & a \\ a & -a-b & b \\ b & a & -a \end{pmatrix}$. Il n'existe pas de couple (a, b) tel que $aA + bB = I_3$ donc $I_3 \notin E$. E n'est pas un sous-anneau.
• Montrons que E est stable par multiplication :
Soit $a, b, a', b' \in \mathbb{R}$.
Par distributivité $(aA + bB)(a'A + b'B) = aa'A^2 + ab'AB + ba'BA + bb'B^2$.
Or le calcul matriciel donne :

$$A^2 = \begin{pmatrix} 1 & 1 & -2 \\ -2 & 1 & 1 \\ 1 & -2 & 1 \end{pmatrix} = -2A + B \in E, \quad B^2 = \begin{pmatrix} 1 & -2 & 1 \\ 1 & 1 & -2 \\ -2 & 1 & 1 \end{pmatrix} = A - 2B \in E,$$

$$AB = \begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix} = -A - B \in E \quad \text{et} \quad BA = \begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix} = AB \in E.$$

On en déduit que $(aA + bB)(a'A + b'B) \in E$.
On remarque de plus que la multiplication induite sur E est commutative.

• Recherche d'un élément neutre

Soit x et $y \in \mathbb{R}$ et $X = xA + yB$.
Si X est neutre pour la multiplication induite sur E, on a en particulir $XA = A$.
Or $XA = xA^2 + yAB = (-2x - y)A + (x - y)B$ et la famille (A, B) est libre :

$$XA = A \iff \begin{cases} -2x - y = 1 \\ \quad x - y = 0 \end{cases} \iff \begin{cases} x = -1/3 \\ y = -1/3 \end{cases}$$

La seule matrice possible est $X = -\frac{1}{3}A - \frac{1}{3}B = \frac{1}{3}\begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix}$

Réciproquement, soit $X = -\frac{1}{3}A - \frac{1}{3}B$. On a vu que $AX = XA = A$.

Et on a $BX = XB = -\frac{1}{3}AB - \frac{1}{3}B^2 = \frac{1}{3}A + \frac{1}{3}B - \frac{1}{3}A + \frac{2}{3}B = B$.
On en déduit que pour toute $M \in E$, $MX = XM = M$. Donc X est neutre pour la multiplication induite sur E.
Donc $(E, +, \times)$ est un anneau.

2) Pour justifier que la matrice A n'est pas inversible, on peut faire remarquer qu'en ajoutant les trois colonnes de A on forme la colonne nulle ou bien calculer le déterminant de A :

$$\det(A) = \begin{vmatrix} -1 & 0 & 1 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{vmatrix} = (-1)\begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} - 1\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = -1 + 1 = 0.$$

Soit $a, b \in \mathbb{R}$ et $M = (aA + bB)$.
On a vu $MA = aA^2 + bBA = (-2a - b)A + (a - b)B$. D'où :

$$\begin{aligned} MA = X &\iff (-2a - b)A + (a - b)B = -\frac{1}{3}A - \frac{1}{3}B \\ &\iff \begin{cases} -2a - b = -1/3 \\ a - b = -1/3 \end{cases} \\ &\iff \begin{cases} a = 0 \\ b = 1/3 \end{cases} \end{aligned}$$

la famille (A, B) est libre

$L_2 - L_1$ donne $a = 0$

La matrice A est admet un inverse dans l'anneau E qui est la matrice $\frac{1}{3}B$.

Exercice 10 *Anneau de Boole*

1) Soit $x \in A$. D'une part $(2x)^2 = (2x)(2x) = 4x^2$. D'autre part, d'après $(\star)$, on a $x^2 = x$ et $(2x)^2 = 2x$ (car $x + x \in A$). Donc $2x = 4x$. Donc $2x = 0$.

2) Soit x et y dans A. D'après $(\star)$, on a $x^2 = x$, $y^2 = y$ et $(x + y)^2 = x + y$. Donc

$$x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$$

On en déduit que $xy + yx = 0$. En ajoutant yx on obtient $xy + 2yx = yx$. Donc, d'après la question précédente, $xy = yx$.
Donc l'anneau A est commutatif.

3) Soit x un élément inversible de A. En multipliant $x^2 = x$ par x^{-1}, on obtient $x = 1_A$.
Réciproquement, l'élément neutre 1_A est bien inversible.
Le seul élément inversible de A est 1_A.

Exercice 11

1) Comme $\left(\overline{a}\right)^n = \overline{a^n} = \overline{N + 1} = \overline{1}$, on a $\overline{a}$ est inversible d'inverse $\left(\overline{a}\right)^{n-1}$.
Le calcul précédent indique également que l'ordre de $\overline{a}$ dans $U(\mathbb{Z}/N\mathbb{Z})$ est un diviseur n.
Puisque $a \geqslant 2$, on a $2 \leqslant a < a^2 < \cdots < a^{n-1} < a^n = N + 1$.
Plus précisément $a^{n-1} = \frac{N+1}{a} \leqslant \frac{N+1}{2} < N$. Donc $\overline{a}, \left(\overline{a}\right)^2, \ldots, \left(\overline{a}\right)^{n-2}$ et $\left(\overline{a}\right)^{n-1}$ sont différents de $\overline{1}$. Donc l'ordre de $\overline{a}$ est exactement égal à n.

2) D'après le cours, $U(\mathbb{Z}/N\mathbb{Z})$ est un groupe de cardinal $\varphi(N)$. Comme l'ordre d'un élément dans un groupe divise le cardinal du groupe, on en déduit que n divise $\varphi(N)$.

CORRECTIONS

Exercice 12

1) Soit $k \in \mathbb{N}^*$. Précisons l'ensemble $\mathcal{D}_0$ des diviseurs de 0 de l'anneau $\mathbb{Z}/2^k\mathbb{Z}$.
Soit $n \in [\![1, 2^k - 1]\!]$.
- Si n est pair alors $2^{k-1}n$ est divisible par 2^k. Donc $\overline{2^{k-1}} \cdot \overline{n} = 0$ dans $\mathbb{Z}/2^k\mathbb{Z}$ et $\overline{n} \in \mathcal{D}_0$.
- Sinon $\overline{n}$ est inversible dans $\mathbb{Z}/2^k\mathbb{Z}$ car n et 2^k sont premiers entre eux donc n'est pas un diviseur de 0.

En conclusion $\mathcal{D}_0 = \{\overline{n}, n \in [\![1, 2^k - 1]\!] \text{ et } n \text{ pair}\} = \left\{\overline{2p}, p \in [\![1, 2^{k-1} - 1]\!]\right\}$.

2) On considère A un anneau commutatif possèdant n diviseurs de zéro, avec $n \geqslant 1$.

a) Soit a un diviseur de 0 et $f : A \to A, x \mapsto ax$.
Pour tous x et y dans A, on a :
$$\begin{aligned} f(x+y) &= a(x+y) && \text{par distributivité de } \times \text{ sur } + \\ &= ax + ay && \text{par définition de } f \\ &= f(x) + f(y) \end{aligned}$$
Donc $f : A \to A, x \mapsto ax$ est un morphisme de groupes de $(A, +)$ dans lui-même.
Soit $y \in \mathrm{Im}(f)$. On sait qu'il existe $x_0 \in A$ tels que $f(x_0) = y$ et qu'en notant A_y l'ensemble des antécédents de y par le morphisme f on a :
$$A_y = \{x_0 + h, h \in \mathrm{Ker}(f)\}.$$
L'application $h \mapsto x_0 + h$ étant bijective de $\mathrm{Ker}(f)$ dans A_y, ces ensembles ont le même cardinal.
On a montré que tout élément de $\mathrm{Im}(f)$ admet exactement $\mathrm{card}\big(\mathrm{Ker}(f)\big)$ antécédents.

b) Avec les notations précédentes, on a $A = \bigcup_{y \in \mathrm{Im}(f)} A_y$ car f est définie sur A.
De plus la réunion est disjointe. On a donc :
$$\begin{aligned} \mathrm{card}(A) &= \sum_{y \in \mathrm{Im}(f)} \mathrm{card}(A_y) && \text{par la question précédente} \\ &= \sum_{y \in \mathrm{Im}(f)} \mathrm{card}\big(\mathrm{Ker}(f)\big) && \text{par définition de } f \\ &= \mathrm{card}\big(\mathrm{Im}(f)\big)\mathrm{card}\big(\mathrm{Ker}(f)\big). \end{aligned}$$

Remarque
On remarquera la similitude avec le théorème du rang.

Si $x \in \mathrm{Ker}(f) \setminus \{0\}$, alors on a $ax = 0$ et $x \neq 0$ donc x est un diviseur de 0.
Donc $\mathrm{card}\big(\mathrm{Ker}(f)\big) \leqslant n + 1$.
Si $y \in \mathrm{Im}(f) \setminus \{0\}$, il existe $x \in A$ tel que $y = ax$. Or, a étant un diviseur de 0, il existe $b \in A \setminus \{0\}$ tel que $ba = 0$. Donc $by = b(ax) = (ba)x = 0$. Il en résulte que y est un diviseur de 0. Donc $\mathrm{card}\big(\mathrm{Im}(f)\big) \leqslant n + 1$.
Compte tenu des trois résultats précédents, A a au plus $(n+1)^2$ éléments.

Remarque
Dans l'exemple de la première question, il y a $n = 2^{k-1} - 1$ diviseurs de 0 et $(n+1)^2 = 2^k$ est exactement le nombre d'éléments de l'anneau $\mathbb{Z}/2^k\mathbb{Z}$.

Exercices avec questions ouvertes

Exercice 13

Si f est un morphisme d'anneaux de $(\mathbb{Z}, +, \times)$ dans lui-même, on a $f(1) = 1$.
On en déduit (voir exercice 1 du chapitre 1) que pour tout $n \in \mathbb{Z}$, $f(n) = f(n1) = nf(1) = n$.
Réciproquement l'identité est un morphisme de $(\mathbb{Z}, +)$ dans lui-même

Exercice 14

Si f est un morphisme d'anneaux de $(\mathbb{R}, +, \times)$ dans lui-même, on a $f(1) = 1$.
On en déduit par une démonstration semblable à celle de l'exercice 2 du chapitre 1 que pour tout $r \in \mathbb{Q}$, $f(q) = f(q1) = qf(1) = q$.
De plus f est croissante car si $x \leqslant y$, on a

$$f(y) - f(x) = f(y - x) = f\left(\sqrt{y - x}^{\,2}\right) = f\left(\sqrt{y - x}\right)^2 \geqslant f(x)$$

Soit $x \in \mathbb{R}$. On sait qu'il existe (approximation décimale des réels) des suites $(m_n)_{n \in \mathbb{N}}$ et $(M_n)_{n \in \mathbb{N}}$ de rationnels* qui convergent vers x et telles que $m_n \leqslant x \leqslant M_n$.
On a alors $m_n = f(m_n) \leqslant f(x) \leqslant f(M_n) = M_n$ et par théorème d'encadrement, $f(x) = x$.
Réciproquement, $\mathrm{Id}_{\mathbb{R}}$ est un morphisme d'anneaux de $(\mathbb{R}, +, \times)$ dans lui-même.
L'identité est le seul morphisme d'anneaux de $(\mathbb{R}, +, \times)$ dans lui-même.

Exercice 15

1) Si la multiplication est commutative, on a pour tous x et y dans A :

$$(xy)^2 = xyxy = xxyy = x^2y^2.$$

2) Montrons que la réciproque est vraie.
On suppose

$$\forall x, y \in A, \quad (xy)^2 = x^2y^2. \qquad (\star)$$

Soit x et y dans A. En utilisant $(\star)$ pour x et $1_A + y$ on a :
$(x + xy)^2 = \left(x(1_A + y)\right)^2 = x^2(1_A + y)^2$.
Or $(x + xy)^2 = x^2 + x^2y + xyx + (xy)^2 = x^2 + x^2y + xyx + x^2y^2$
et $x^2(1_A + y)^2 = x^2(1_A + 2y + y^2) = x^2 + 2x^2y + x^2y^2$.
Donc $2x^2y = x^2y + xyx$ puis $x^2y = xyx$.
Cette dernière relation étant vraie pour tous x dans A, on peut utiliser $1_A + x$ et on obtient $(1_A + x)^2y = (1_A + x)y(1_A + x)$.
Or d'une part : $(1_A + x)^2y = (1_A + 2x + x^2)y = y + 2xy + x^2y = y + 2xy + xyx$,
et d'autre part : $(1_A + x)y(1_A + x) = (y + xy)(1_A + x) = y + yx + xy + xyx$.
On en déduit $yx + xy = 2xy$ donc $yx = xy$.
L'anneau est effectivement commutatif.

*Par exemple $m_n = \lfloor 10^n x \rfloor / 10^n$ et $M_n = m_n + 10^{-n}$.

Algèbre (révisions) 3

Exercices axés sur le calcul

Exercice 1 *Polynômes de Legendre*

1) Soit $P \in \mathbb{R}[X]$, a et b deux racines de P de multiplicité $m \in \mathbb{N}^*$ telles que $a < b$.
Montrer que pour tout $k \in [\![1, m]\!]$, $P^{(k)}$ admet au moins k racines dans $]a, b[$.

2) Pour $n \in \mathbb{N}^*$, on note $Q_n = (X^2 - 1)^n$ et $L_n = Q_n^{(n)}$.
   a) Quel est le degré de L_n ?
   b) Montrer que L_n admet exactement n racines et qu'elles sont toutes dans $]-1, 1[$.

D'après Mines-Télécom

Exercice 2 *Somme et produit des racines d'un polynôme, transformation de* $\mathrm{e}^{\mathrm{i}\,\theta} \pm 1$

Soit $n \in \mathbb{N}^*$. On note $P_n = 1 + X + \cdots + X^n$.

1) Justifier que P_n admet n racines éventuellement confondues dans $\mathbb{C}$.
2) Préciser le produit et la somme de ces racines.
3) Résoudre $P_n(z) = 0$. Contrôler les résultats du 2).
4) Déduire de $P(1)$ la valeur de $\prod_{k=1}^{n} \sin\left(\frac{k\pi}{n+1}\right)$.

Exercices axés sur le raisonnement

Exercice 3 *Formule du binôme, unicité des coefficients d'un polynôme*

Pour $n \in \mathbb{N}$, on note $S_n = \sum_{k=0}^{n} \binom{n}{k}^2$.

Déterminer la valeur de S_n en utilisant le coefficient de X^n dans $(1+X)^n(1+X)^n$.

Exercice 4

Dans l'espace vectoriel des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, on considère pour $n \in \mathbb{N}^*$, la fonction :

$$f_n : x \mapsto \mathrm{e}^{x/n}.$$

Montrer que la famille $(f_n)_{n\in\mathbb{N}^*}$ est libre.

Exercice 5

Soit E un $\mathbb{K}$-espace vectoriel, f un endomorphisme de E et $a \in \mathbb{K} \setminus \{0\}$.
On suppose que $f^3 - 3af^2 + a^2 f = 0$.
Montrer que $E = \mathrm{Ker}(f) \oplus \mathrm{Im}(f)$.

D'après Mines-Télécom

Exercice 6 *Fréquent*

Soit E un $\mathbb{K}$-espace vectoriel et $f_1, f_2, \dots, f_n$ des endomorphismes de E.
On suppose que $f_1 + f_2 + \cdots + f_n = \mathrm{Id}_E$ et :

$$\forall i, j \in [\![1, n]\!], \quad i \neq j \Longrightarrow f_i \circ f_j = 0.$$

1) Montrer que pour tout $i \in [\![1, n]\!]$, f_i est une projection vectorielle.

2) Montrer que $\bigoplus_{i=1}^{n} \mathrm{Im}(f_i) = E$.

Exercice 7 *Classique*

Soit E un espace vectoriel et p, q des projecteurs de E.

1) Montrer que $p + q$ est un projecteur si, et seulement si, $p \circ q = q \circ p = 0$.

2) Dans ce cas, montrer que $\mathrm{Ker}(p+q) = \mathrm{Ker}(p) \cap \mathrm{Ker}(q)$ et $\mathrm{Im}(p+q) = \mathrm{Im}(p) \oplus \mathrm{Im}(q)$.

D'après CCINP

Exercice 8

Soit E et F deux $\mathbb{K}$-espaces vectoriels, $u \in \mathcal{L}(E, F)$ et $v \in \mathcal{L}(F, E)$. On suppose que

$$u = u \circ v \circ u \quad \text{et} \quad v = v \circ u \circ v.$$

Montrer que

$$E = \mathrm{Ker}(u) \oplus \mathrm{Im}(v).$$

D'après Mines-Télécom

Exercice 9

Soit u un endomorphisme d'un $\mathbb{K}$-espace vectoriel E. On suppose que l'endomorphisme u est nilpotent d'indice p c'est-à-dire que $u^p = 0$ et $u^{p-1} \neq 0$. On note $\mathrm{e}^u = \sum_{k=0}^{p-1} \frac{1}{k!} u^k$.

1) Soit $x \in E$ et $k \in \mathbb{N}^*$ tel que $u^k(x) \neq 0_E$.
Montrer que la famille $\big(x, u(x), u^2(x), \dots, u^k(x)\big)$ est libre.

2) Déterminer $\mathrm{Ker}(\mathrm{e}^u - \mathrm{Id}_E)$.

D'après Mines-Télécom

Exercice 10

Soit $n \in \mathbb{N}$ et $E = \mathbb{R}_n[X]$.
Pour tout $i \in [\![0, n]\!]$, on note

$$F_i = \{P \in E \mid \forall j \in [\![0, n]\!] \setminus \{i\}, P(j) = 0\}.$$

Montrer que les F_i sont des sous-espaces vectoriels et que $E = \bigoplus_{i=1}^{n} F_i$.

Exercice 11 ⋆

Soit E un $\mathbb{K}$-espace vectoriel de dimension $n \in \mathbb{N} \setminus \{0, 1\}$.
On note $\mathcal{B} = (e_i)_{1 \leqslant i \leqslant n}$ une base de E.
Pour $i \in [\![1, n]\!]$, on pose :

$$G_i = \mathrm{vect}(e_1, \dots, e_{i-1}, e_{i+1}, \dots, e_n) \quad \text{et} \quad H_i = \{f \in \mathcal{L}(E) \mid G_i \subset \mathrm{Ker}(f)\}.$$

1) Soit $i \in [\![1, n]\!]$. Montrer que H_i est un sous-espace vectoriel de $\mathcal{L}(E)$.

2) Montrer que : $\bigoplus_{i=1}^{n} H_i = \mathcal{L}(E)$.

Exercice 12

Soit $n \in \mathbb{N}^*$ et $H_1, H_2, \dots, H_k$ des hyperplans d'un espace vectoriel E de dimension n.
Montrer que $\dim\left(\bigcap_{i=1}^{k} H_i\right) \geqslant n - k$.

Exercices avec questions ouvertes

Exercice 13

Peut-on trouver deux endomorphismes non nuls de $\mathbb{R}^2$ vérifiant :

1) $\mathrm{rg}(u + v) < \mathrm{rg}(u) + \mathrm{rg}(v)$

2) $\mathrm{rg}(u + v) = \mathrm{rg}(u) + \mathrm{rg}(v)$

3) $\mathrm{rg}(u + v) > \mathrm{rg}(u) + \mathrm{rg}(v)$.

Exercice 14

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie et $F_1, \dots, F_n$ des sous-espaces vectoriels de E tels que $E = F_1 + \cdots + F_n$.
Existe-t-il des sous-espaces vectoriels $G_1, \dots, G_n$ tels que pour tout $i \in [\![1, n]\!]$, $G_i \subset F_i$ et $E = \bigoplus_{i=1}^{n} G_i$?

Corrections

Exercices axés sur le calcul

Exercice 1

1) Pour $k \in [\![1,m]\!]$, on note $\mathcal{P}_k$: « $P^{(k)}$ admet au moins k racines dans $]a,b[$ ».
   - P étant un polynôme, il est en particulier continu sur $[a,b]$ et dérivable sur $]a,b[$.
     Comme $P(a) = 0$ et $P(b) = 0$, on a $P(a) = P(b)$.
     Donc le théorème de Rolle assure que P' s'annule au moins une fois sur $]a,b[$.
     Donc $\mathcal{P}_1$ est vraie.
   - Soit $k \in [\![1,m-1]\!]$. On suppose $\mathcal{P}_k$ vraie.
     On dispose, en les rangeant dans l'ordre croissant, de racines $x_1 < \cdots < x_k$ de $P^{(k)}$ dans $]a,b[$. a et b étant des racines de multiplicité m, elles sont aussi racines de $P^{(k)}$ (car $k \leqslant m-1$). On note $x_0 = a$ et $x_{k+1} = b$. Pour $i \in [\![0,k]\!]$, le théorème de Rolle appliqué à $P^{(k)}$ sur $[x_i, x_{i+1}]$ assure qu'il existe une racine $c_i \in]x_i, x_{i+1}[$ de $P^{(k+1)}$. En choisissant un de ces points c_i dans chacun des intervalles $]x_i, x_{i+1}[$, on obtient des points distincts car :

$$x_0 < c_0 < x_1 < c_1 < x_2 < \cdots < x_k < c_k < x_{k+1}.$$

     On a donc au moins $k+1$ racines distinctes dans $]a,b[$ pour $P^{(k+1)}$.
     Donc $\mathcal{P}_{k+1}$ est vraie.

   On a montré par récurrence que $\mathcal{P}_k$ est vraie pour tout k$\in [\![1,m]\!]$.

2) a) $(X^2-1)^n$ est de degré $2n$ et sa dérivée n-ième est donc de degré n.

   b) Étant de degré n, L_n admet au plus n racines distinctes.
   D'autre part, $(X^2-1)^n = (X-1)^n(X+1)^n$ donc 1 et -1 sont racines de multiplicité n de Q_n. La question précédente montre que L_n admet n racines distinctes dans $]-1,1[$.
   Donc L_n admet exactement n racines et elles sont toutes dans $]-1,1[$.

Exercice 2

1) On a $\deg P_n = n$ donc P_n admet n racines (éventuellement confondues) dans $\mathbb{C}$.

2) Puisque le coefficient dominant de P_n est 1, on a, en notant $z_1, z_2, \ldots, z_n$ les racines de P_n, $P_n = 1 \prod_{k=1}^{n} (X - z_k)$ et le cours assure que :

$$P_n = X^n - sX^{n-1} + \cdots + (-1)^n p.$$

   Donc, par unicité des coefficients d'un polynôme, $s = -1$ et $p = (-1)^n$.

3) 1 n'est pas racine de P_n et on sait que pour $z \neq 1$, $1 + z + \cdots + z^n = \frac{1-z^{n+1}}{1-z}$ (somme de termes consécutifs d'une suite géométrique). Donc :
   $P_n(z) = 0 \iff (z^{n+1} = 1 \text{ et } z \neq 1)$.
   Les racines de P_n sont les $z_k = \exp\left(\frac{2ik\pi}{n+1}\right)$ pour $k \in [\![1,n]\!]$.

En notant $\omega = \exp\left(\frac{2\mathrm{i}\pi}{n+1}\right)$. On a $\omega \neq 1$, $z_k = \omega^k$ et $\omega^{n+1} = 1$. D'où les calculs suivants :

$$s = \sum_{k=1}^{n} z_k = \sum_{k=1}^{n} \omega^k = \omega \frac{1-\omega^n}{1-\omega} = \frac{\omega - \omega^{n+1}}{1-\omega} = \frac{\omega - 1}{1-\omega} = -1$$

$$p = \prod_{k=1}^{n} z_k = \prod_{k=1}^{n} \omega^k = \omega^{1+2+\cdots+n} = \omega^{\frac{n(n+1)}{2}} = \exp(\mathrm{i}n\pi) = (-1)^n.$$

4) D'une part, par la forme développée de P_n, on a $P_n(1) = n+1$.

D'autre part, par la forme factorisée de P_n, on a $P_n(1) = \prod\limits_{k=1}^{n}\left(1 - \exp\left(\frac{2\mathrm{i}k\pi}{n+1}\right)\right)$.

Or $1 - \mathrm{e}^{\mathrm{i}\theta} = \mathrm{e}^{\mathrm{i}\theta/2}\big(-2\mathrm{i}\sin(\theta/2)\big)$ donc, en notant $\theta_k = \frac{2k\pi}{n+1}$:

$$\begin{aligned}
\prod_{k=1}^{n} \mathrm{e}^{\mathrm{i}\theta_k/2}(-2\mathrm{i}) &= (-2\mathrm{i})^n \prod_{k=1}^{n} \mathrm{e}^{\mathrm{i}\theta_k/2} && \mathrm{e}^a\mathrm{e}^b = \mathrm{e}^{a+b} \\
&= (-2\mathrm{i})^n\, \mathrm{e}^{\frac{\mathrm{i}}{2}\left(\sum\limits_{k=1}^{n}\theta_k\right)} && \sum_{k=1}^{n} k = \frac{n(n+1)}{2} \\
&= (-2\mathrm{i})^n\, \mathrm{e}^{\mathrm{i}\,n\pi/2} && \mathrm{e}^{\mathrm{i}\pi/2} = \mathrm{i} \\
&= (-2\mathrm{i})^n(\mathrm{i}^n) && \mathrm{i}^2 = -1 \\
&= 2^n.
\end{aligned}$$

Donc

$$\prod_{k=1}^{n} \sin\left(\frac{k\pi}{n+1}\right) = \frac{n+1}{2^n}.$$

Exercices axés sur le raisonnement

Exercice 3

D'après la formule du binôme de Newton :

$$(1+X)^n = \sum_{k=0}^{n}\binom{n}{k}X^k, \quad (1+X)^{2n} = \sum_{k=0}^{2n}\binom{2n}{k}X^k$$

D'une part, le coefficient de X^n dans $(1+X)^{2n}$ est $\binom{2n}{n}$.

D'autre part, le coefficient de X^n dans le produit $(1+X)^n(1+X)^n$ est $\sum\limits_{k=0}^{n}\binom{n}{k}\binom{n}{n-k}$.

De plus, on sait que $\binom{n}{n-k} = \binom{n}{k}$ donc par unicité des coefficients :

$$\sum_{k=0}^{n}\binom{n}{k}^2 = \binom{2n}{n}.$$

Remarque

Ce résultat est obtenu autrement à l'exercice 8 du chapitre 27.

Exercice 4

Pour $n \in \mathbb{N}^*$, on note $\mathcal{P}_n$: « la famille $(f_1, f_2, \dots, f_n)$ est libre ».

- Pour $n = 1$, $\mathcal{P}_1$ est vraie car f_1 n'est pas la fonction nulle.
- Soit $n \in \mathbb{N}^*$. On suppose $\mathcal{P}_n$ vraie.
  Soit $a_1, a_2, \dots, a_n$ des réels tels que

$$a_1 f_1 + a_2 f_2 + \cdots + a_n f_n + a_{n+1} f_{n+1} = 0 \qquad (\star)$$

• Méthode 1 (par dérivation)

En dérivant $(\star)$ on obtient :

$$a_1 f_1 + \cdots + \frac{1}{n} a_n f_n + \frac{1}{n+1} a_{n+1} f_{n+1} = 0 \qquad (\star\star)$$

En formant $(\star)$-$(n+1)(\star\star)$, on obtient :

$$a_1(1 - n - 1) f_1 + \cdots + a_n \left(1 - \frac{n+1}{n}\right) f_n = 0.$$

La famille $(f_1, f_2, \dots, f_n)$ étant libre d'après $\mathcal{P}_n$, on a pour $k \in [\![1, n]\!]$ $a_k \frac{k-(n+1)}{k} = 0$, donc $a_k = 0$.

Il reste donc $a_{n+1} f_{n+1} = 0$. Or f_{n+1} n'est pas la fonction nulle donc $a_{n+1} = 0$.

• Méthode 2 (par une limite)

En évaluant $(\star)$ en $x \in \mathbb{R}$, on a $\sum\limits_{k=1}^{n+1} a_k \mathrm{e}^{x/k} = 0$ puis, en divisant par $\mathrm{e}^{x/(n+1)} \neq 0$ et en utilisant $\frac{\mathrm{e}^{x/k}}{\mathrm{e}^{x/(n+1)}} = \mathrm{e}^{x/k - x/(n+1)}$, $\sum\limits_{k=1}^{n+1} a_k \mathrm{e}^{x/k - x/(n+1)} = 0$.

Pour $k \in [\![1, n]\!]$, $\frac{1}{k} - \frac{1}{n+1} = \frac{(n+1)-k}{k(n+1)} > 0$ donc $\lim\limits_{x \to -\infty} \mathrm{e}^{x/k - x/(n+1)} = 0$.

Donc $\lim\limits_{x \to -\infty} \sum\limits_{k=1}^{n+1} a_k \mathrm{e}^{x/k - x/(n+1)} = 0 + a_{n+1}$. Par unicité de la limite $a_{n+1} = 0$.

La relation $(\star)$ devient $\sum\limits_{k=1}^{n} a_k f_k = 0$ et comme $(f_1, f_2, \dots, f_n)$ est libre d'après $\mathcal{P}_n$, on a pour $k \in [\![1, n]\!]$, $a_k = 0$.

Donc pour tout $k \in [\![1, n+1]\!]$, $a_k = 0$. On a montré que la famille $(f_1, f_2, \dots, f_{n+1})$ est libre. Donc $\mathcal{P}_{n+1}$ est vraie.

On a montré par récurrence que pour tout $n \in \mathbb{N}^*$, $\mathcal{P}_n$ est vraie.

Pour toute sous-famille finie $\mathcal{F}$ de $(f_n)_{n \in \mathbb{N}^*}$, il existe un rang $n \in \mathbb{N}^*$, tel que $\mathcal{F}$ est une sous-famille de $(f_1, f_2, \dots, f_n)$. Donc $\mathcal{F}$ est libre comme sous-famille d'une famille libre.

Donc la famille $(f_n)_{n \in \mathbb{N}^*}$ est libre.

Exercice 5

• La somme de l'image et du noyau est directe

Soit $x \in \mathrm{Ker}(f) \cap \mathrm{Im}(f)$.

Il existe z tel que $x = f(z)$ et $f(x) = 0_E$. Donc $f^2(z) = 0_E$ et $f^3(z) = 0_E$.

Puisque $(f^3 - 3af^2 + a^2 f)(z) = 0_E$, on a $a^2 x = 0_E$. Comme $a \neq 0$, on trouve $x = 0_E$.
La somme $\operatorname{Ker} f + \operatorname{Im} f$ est directe.

• *Décomposition*

Soit $x \in E$.

Analyse Supposons que $x = u + v$ avec $u \in \operatorname{Ker}(f)$ et $v = f(w) \in \operatorname{Im}(f)$.
On a alors $f(x) = f^2(w)$ et $f^2(x) = f^3(w) = 3af^2(w) - a^2 f(w)$ (car $f^3 = 3af^2 - a^2 f$).
Donc $f^2(x) = 3af(x) - a^2 v$ et $v = \frac{1}{a^2}\big(3af(x) - f^2(x)\big)$.

Synthèse On pose $v = \frac{1}{a^2}\big(3af(x) - f^2(x)\big)$ et $u = x - v$.
On a alors $x = u + v$ et $v \in \operatorname{Im}(f)$ car c'est l'image par f du vecteur $\frac{1}{a^2}\big(3ax - f(x)\big)$. Et :
$f(u) = f(x) - f(v) = f(x) - \frac{1}{a^2}\big(3af^2(x) - f^3(x)\big) = \frac{1}{a^2}\big(a^2 f(x) - 3af^2(x) + f^3(x)\big) = 0_E$
ce qui prouve que $u \in \operatorname{Ker}(f)$.

Les deux sous-espaces $\operatorname{Ker}(f)$ et $\operatorname{Im}(f)$ sont supplémentaires dans E.

Remarque
Lorsque E est de dimension finie, on a alors directement $E = \operatorname{Ker}(f) \bigoplus \operatorname{Im}(f)$ car le théorème du rang donne $\dim \operatorname{Ker}(f) + \dim \operatorname{Im}(f) = \dim(E)$.

Exercice 6

1) Soit $i \in [\![1,n]\!]$. $f_i \in \mathcal{L}(E)$ et, puisque $\circ$ est distributive sur $+$ dans $\mathcal{L}(E)$, on a :

$$f_i \circ (f_1 + f_2 + \cdots + f_n) = \sum_{k=1}^{n} f_i \circ f_k = 0 + f_i \circ f_i.$$

Or $f_1 + f_2 + \cdots + f_n = \operatorname{Id}_E$ et $f_i \circ \operatorname{Id}_E = f_i$ donc $f_i = f_i^2$ et f_i est une projection.

2) **• *La somme*** $\sum_{i=1}^{n} \operatorname{Im}(f_i)$ ***est directe***

Soit $(x_1, x_2, \ldots, x_n) \in \prod_{i=1}^{n} \operatorname{Im}(f_i)$ tel que $\sum_{i=1}^{n} x_i = 0_E$ $(\star)$.
Soit $k \in [\![1,n]\!]$. Par linéarité de f_k, on a $f_k(0_E) = 0_E$ et :

$$\begin{aligned} f_k\left(\sum_{i=1}^{n} x_i\right) &= \sum_{i=1}^{n} f_k(x_i) \\ &\quad \text{Im}(f_i) \subset \operatorname{Ker}(f_k) \text{ pour } k \neq i \text{ car } f_k \circ f_i = 0 \\ &= 0 + f_k(x_k) \\ &\quad \operatorname{Im}(f_k) = \operatorname{Ker}(f_k - \operatorname{Id}_E) \text{ car } f_k \text{ projection} \\ &= x_k. \end{aligned}$$

On a donc $x_k = 0_E$.
Cela étant valable pour tout $k \in [\![1,n]\!]$, on a montré que la somme est directe.

• *La somme* $\sum_{i=1}^{n} \operatorname{Im}(f_i)$ ***est égale à*** E

$\subset$ Pour tout $i \in [\![1,n]\!]$, $\operatorname{Im}(f_i)$ est un sous-espace de E donc $\sum_{i=1}^{n} \operatorname{Im}(f_i) \subset E$.

$\supset$ Soit $x \in E$, on a $x = \operatorname{Id}_E(x) = f_1(x) + f_2(x) + \cdots + f_n(x) \in \sum_{i=1}^{n} \operatorname{Im}(f_i)$.

Donc $E \subset \sum_{i=1}^{n} \mathrm{Im}(f_i)$.

On a montré par double inclusion que $\sum_{i=1}^{n} \mathrm{Im}(f_i) = E$.

Compte tenu des deux résultats, $\bigoplus_{i=1}^{n} \mathrm{Im}(f_i) = E$.

Exercice 7

1) $p+q$ est un endomorphisme de E car p et q le sont.
On a $(p+q)^2 = p^2 + q^2 + p \circ q + q \circ p = p + q + p \circ q + q \circ p$.

- Si $p \circ q = q \circ p = 0$, alors on a immédiatement $(p+q)^2 = p+q$ et $p+q$ est un projecteur.
- Si $p+q$ est un projecteur, alors $p \circ q + q \circ p = 0$. Et en composant par p à droite et à gauche :

$$p \circ q + p \circ q \circ p = 0 \quad \text{et} \quad p \circ q \circ p + q \circ p = 0$$

ce qui donne $p \circ q = q \circ p$ puis, comme $p \circ q = -q \circ p$, $p \circ q = q \circ p = 0$.

2) • ***Noyau de*** $p+q$

$\subset$ Si $x \in \mathrm{Ker}(p) \cap \mathrm{Ker}(q)$ alors $(p+q)(x) = p(x) + q(x) = 0_E$ donc $x \in \mathrm{Ker}(p+q)$.

$\supset$ Si $x \in \mathrm{Ker}(p+q)$, on a $p(x) = -q(x)$. On déduit en prenant l'image par p que $p^2(x) = -p \circ q(x) = 0_E$. Or, p étant un projecteur, on a $p^2 = p$. Donc $p(x) = 0$ et $x \in \mathrm{Ker}(p)$. Comme $q(x) = -p(x) = 0_E$, on a aussi $x \in \mathrm{Ker}(q)$.
Finalement $x \in \mathrm{Ker}(p) \cap \mathrm{Ker}(q)$.

On a montré par double inclusion :

$$\mathrm{Ker}(p) \cap \mathrm{Ker}(q) = \mathrm{Ker}(p+q).$$

• ***Image de*** $p+q$

Rappelons que l'image d'un projecteur est l'ensemble des vecteurs invariants par ce projecteur.
Si $x \in \mathrm{Im}(p) \cap \mathrm{Im}(q)$, on a $p(x) = x$ et $q(x) = x$.
Donc $0_E = p \circ q(x) = p\big(q(x)\big) = p(x) = x$.
On a montré que la somme $\mathrm{Im}(p) + \mathrm{Im}(q)$ est directe.

$\subset$ Si $x \in \mathrm{Im}(p+q)$, alors $x = (p+q)(x) = p(x) + q(x)$ donc $x \in \mathrm{Im}(p) \oplus \mathrm{Im}(q)$.

$\supset$ Si $x \in \mathrm{Im}(p) \oplus \mathrm{Im}(q)$, on a $x = y + z$ avec $y \in \mathrm{Im}(p)$ et $z \in \mathrm{Im}(q)$. Comme $p \circ q = 0$, on a $\mathrm{Im}(q) \subset \mathrm{Ker}(p)$. Donc $p(z) = 0_E$. Ainsi $p(x) = p(y) + q(z) = y + 0 = y$.
De même, on déduit de $q \circ p = 0$ que $q(x) = z$. Ainsi $(p+q)(x) = p(x) + q(x) = y + z = x$ et $x \in \mathrm{Im}(p+q)$.

On a montré par double inclusion :

$$\mathrm{Im}(p+q) = \mathrm{Im}(p) \oplus \mathrm{Im}(q).$$

Exercice 8

Soit $x \in E$.

- ***Unicité de décomposition***

Supposons $x = y + z$ avec $y \in \operatorname{Ker}(u)$ et $z \in \operatorname{Im}(v)$. Il existe $t \in F$ tel que $z = v(t)$ et $u(y) = 0_E$.

On a alors par linéarité :

$u(x) = 0_E + u(z) = u \circ v(t)$, puis $v \circ u(x) = v \circ u \circ v(t) = v(t) = z$. D'où on déduit $z = v \circ u(x)$ et $y = x - v \circ u(x)$. Cela montre l'unicité de la décomposition d'un vecteur de E et donc le caractère direct de la somme.

- ***Existence de décomposition***

On pose $z = v \circ u(x)$ et $y = x - v \circ u(x)$. On a $x = y + z, z = v\big(u(x)\big) \in \operatorname{Im}(v)$. Et par linéarité : $u(y) = u(x) - u \circ v \circ u(x) = 0_F$ car $u = u \circ v \circ u$. Donc $y \in \operatorname{Ker}(u)$.

On a montré $E = \operatorname{Ker}(u) \bigoplus \operatorname{Im}(v)$.

Exercice 9

1) Soit $x \in E$ et $k \in \mathbb{N}^*$ tel que $u^k(x) \neq 0_E$.

Soit $a_0, a_1, \dots, a_k$ des scalaires tels que

$$a_0 x + a_1 u(x) + \cdots + a_k u^k(x) = 0_E \tag{$\star$}$$

On sait que $u^p(x) = 0_E$ donc $u^i(x) = 0_E$ pour tout $i \geqslant p$. Donc $k \leqslant p - 1$. Notons q le plus grand entier tel que $u^q(x) \neq 0_E$. Puisqu'on a $u^i(x) = 0_E$ pour tout $i \geqslant q$, on obtient en prenant l'image de $(\star)$ par u^q (qui est linéaire) : $a_0 u^q(x) = 0_E$. Or $u^q(x) \neq 0_E$ donc $a_0 = 0$.

En prenant alors l'image par u^{q-1} de $(\star)$, on obtient de même $a_1 u^q(x) = 0_E$ donc $a_1 = 0$.

De proche en proche, tous les coefficients $a_0, a_1, \dots, a_k$ sont nuls.

On a montré que la famille $\big(x, u(x), u^2(x), \dots, u^k(x)\big)$ est libre.

2) On a $\mathrm{e}^u - \mathrm{Id}_E = \sum\limits_{k=1}^{p-1} \frac{1}{k!} u^k$ et on va montrer que $\operatorname{Ker}(\mathrm{e}^u - \mathrm{Id}_E) = \operatorname{Ker}(u)$.

$\supset$ Soit $x \in \operatorname{Ker}(u)$. On a $u^k(x) = 0_E$ pour tout $k \in \mathbb{N}^*$ donc $(\mathrm{e}^u - \mathrm{Id}_E)(x) = 0_E$ et $x \in \operatorname{Ker}(\mathrm{e}^u - \mathrm{Id}_E)$.

On a ainsi montré $\operatorname{Ker}(u) \subset \operatorname{Ker}(\mathrm{e}^u - \mathrm{Id}_E)$.

$\subset$ Soit $x \in \operatorname{Ker}(\mathrm{e}^u - \mathrm{Id}_E)$. On a $\sum\limits_{k=1}^{p-1} \frac{1}{k!} u^k(x) = 0_E$.

On raisonne par l'absurde. On suppose que $u(x) \neq 0_E$.

Notons q le plus grand entier tel que $u^q(x) \neq 0_E$. On a $q \leqslant p - 1$ et la somme ci-dessus devient $\sum\limits_{k=1}^{q} \frac{1}{k!} u^k(x) = 0_E$. Or Or d'après la question précédente la famille $\big(x, u(x), u^2(x), \dots, u^q(x)\big)$ est libre donc la sous-famille $\big(u(x), u^2(x), \dots, u^k(x)\big)$ est libre ce qui contredit l'égalité $\sum\limits_{k=1}^{q} \frac{1}{k!} u^k(x) = 0_E$.

Donc $u(x) = 0_E$ et $x \in \operatorname{Ker}(u)$.

Donc $\operatorname{Ker}(\mathrm{e}^u - \mathrm{Id}_E) \subset \operatorname{Ker}(u)$.

On a montré par double inclusion que $\operatorname{Ker}(\mathrm{e}^u - \mathrm{Id}_E) = \operatorname{Ker}(u)$.

CORRECTIONS

Exercice 10

On peut montrer que les F_i sont des sous-espaces vectoriels en montrant qu'ils contiennent le polynôme nul et sont stables par combinaison linéaire, mais il est plus utile pour la suite d'introduire :

$$\forall i \in [\![0,n]\!], \quad L_i = \prod_{j\in[\![0,n]\!]\setminus\{i\}} (X-j).$$

On a ainsi pour tout $P \in E$:

$$\begin{aligned} P \in F_i &\iff \forall j \in [\![0,n]\!] \setminus \{i\}, P(j) = 0 \\ &\iff L_i \mid P \\ &\iff \exists \alpha \in \mathbb{K}, P = \alpha L_i \\ &\iff P \in \operatorname{vect}(L_i). \end{aligned}$$

les racines sont distinctes

$\deg P \leqslant n, \deg L_i = n$

Ainsi $F_i = \operatorname{vect}(L_i)$ et, en particulier, F_i est un sous-espace vectoriel.

• La somme est directe

Soit $(P_0, P_1, \dots, P_n)$ un élément de $\prod_{k=0}^{n} F_k$ tel que $P_0 + P_1 + \cdots + P_n = 0$ $(\star)$.
Soit $i \in [\![0,n]\!]$. Par définition, i est racine de P_k pour tout $k \neq i$. Donc, en évaluant $(\star)$ en i, on obtient $P_i(i) = 0$. Donc P_i admet $n+1$ racines distinctes. Or $\deg P_i \leqslant n$ donc $P_i = 0$.
Cela étant valable pour tout $i \in [\![0,n]\!]$, on a montré que la somme est directe.

• La somme est égale à E

Puisque la somme est directe, sa dimension est la somme des dimensions de F_i.
Or $F_i = \operatorname{vect}(L_i)$ et $L_i \neq 0$, donc $\dim F_i = 1$.

$$\dim \bigoplus_{i=0}^{n} F_i = \sum_{i=0}^{n} \dim F_i = n+1 = \dim E.$$

Donc $\bigoplus_{i=0}^{n} F_i = E$.

Exercice 11

1) Soit $i \in [\![1,n]\!]$.
   - H_i est une partie de $\mathcal{L}(E)$ qui contient l'endomorphisme nul.
   - Soit $f, g \in H_i$, α et β des scalaires.
     Pour tout $x \in G_i$, on a $f(x) = 0$ (car $G_i \subset \operatorname{Ker}(f)$) et $g(x) = 0$ (de même).
     D'où $(\alpha f + \beta g)(x) = \alpha f(x) + \beta g(x) = 0$ donc $x \in \operatorname{Ker}(\alpha f + \beta g)$.
     Cela prouve que $G_i \subset \operatorname{Ker}(\alpha f + \beta g)$ donc que $(\alpha f + \beta g) \in H_i$.

   Donc H_i est un sous-espace vectoriel de $\mathcal{L}(E)$.

2) ***• La somme est directe***

   Soit $(f_1, f_2, \dots, f_n)$ un élément de $\prod_{i=1}^{n} H_i$ tel que $f_1 + f_2 + \cdots + f_n = 0_{\mathcal{L}(E)}$ $(\star)$.
   Soit $i \in [\![1,n]\!]$. Pour tout $k \in [\![1,n]\!] \setminus \{i\}$, $e_i \in G_k$ donc $f_k(e_i) = 0_E$. En utilisant $(\star)$ pour e_i, on obtient donc $f_i(e_i) = 0_E$. Comme f_i est également nul pour tous les autres vecteurs de base $\mathcal{B}$, on a $f_i = 0_{\mathcal{L}(E)}$.
   On a montré que la somme $\sum_{i=1}^{n} H_i$ est directe.

• *Dimension de H_i*

Soit $i \in [\![1,n]\!]$. Considérons $\Psi : H_i \to E, f \mapsto f(e_i)$.

- Les lois usuelles montrent que Ψ est linéaire.
- Ψ est injective car si $f \in \mathrm{Ker}(\psi)$, alors $f \in H_i$ et $f(e_i) = 0_E$ donc f est nulle sur la base $\mathcal{B}$ d'où f est l'application nulle.
- Montrons que Ψ est surjective.
  Soit $u \in E$. $\mathcal{B}$ étant une base de E, on sait qu'il existe une (et une seule) $f \in \mathcal{L}(E)$ telle que $f(e_k) = 0_E$ pour $k \neq i$ et $f(e_i) = u$. Cette application f appartient à H_i.
  Donc u admet un antécédent par Ψ.

Donc Ψ est un isomorphisme de H_i sur E. Donc $\dim H_i = \dim E$.

• *Conclusion*

Puisque la somme est directe $\dim \bigoplus_{i=1}^{n} H_i = \sum_{i=1}^{n} \dim H_i = \sum_{i=1}^{n} n = n^2$.

Or $\dim \mathcal{L}(E) = \left(\dim E\right)^2 = n^2$, donc $\dim \bigoplus_{i=1}^{n} H_i = \dim \mathcal{L}(E)$. Finalement $\bigoplus_{i=1}^{n} H_i = \mathcal{L}(E)$.

Exercice 12

En utilisant une base de E et des équations de chacun des hyperplans H_i, l'intersection $\bigcap_{i=1}^{k} H_i$ est l'ensemble des vecteurs dont les coordonnées vérifient un système linéaire homogène de k équations (une par hyperplan) et n inconnues (les n coordonnées). Le système étant de rang au plus k, l'ensemble des solutions est de dimension au moins $n - k$.

On a ainsi $\dim \left(\bigcap_{i=1}^{k} H_i \right) \geqslant n - k$.

Exercices avec questions ouvertes

Exercice 13

1) En choisissant par exemple $u = v = \mathrm{Id}_{\mathbb{R}^2}$, on a :

$$\mathrm{rg}(u+v) = \mathrm{rg}(2\mathrm{Id}_{\mathbb{R}^2}) = 2 < 4 = \mathrm{rg}(u) + \mathrm{rg}(v).$$

2) On peut obtenir $\mathrm{rg}(u+v) = \mathrm{rg}(u) + \mathrm{rg}(v)$ en choisissant u et v de rang 1 tel que $u+v$ soit un automorphisme de $\mathbb{R}^2$.
   Par exemple on peut proposer $u : (x,y) \mapsto (x,0)$ (la projection orthogonale sur l'axe Ox), $v : (x,y) \mapsto (0,y)$ (la projection orthogonale sur l'axe Oy). u et v sont de rang 1 et leur somme est l'identité de $\mathbb{R}^2$ qui est de rang 2.

3) On va montrer que « $\mathrm{rg}(u+v) > \mathrm{rg}(u) + \mathrm{rg}(v)$ » est impossible.
   On a $\mathrm{Im}(u+v) \subset \mathrm{Im}(u) + \mathrm{Im}(v)$ donc $\mathrm{rg}(u+v) \leqslant \dim\big(\mathrm{Im}(u) + \mathrm{Im}(v)\big)$. Or la dimension d'une somme est toujours inférieure à la somme des dimensions donc :

$$\mathrm{rg}(u+v) \leqslant \dim\big(\mathrm{Im}(u) + \mathrm{Im}(v)\big) \leqslant \dim \mathrm{Im}(u) \dim \mathrm{Im}(v) = \mathrm{rg}(u) + \mathrm{rg}(v).$$

Exercice 14

On va montrer le résultat par récurrence. Pour $n \in \mathbb{N}^*$, on note $\mathcal{P}_n$: « si $F_1, \dots, F_n$ sont des sous-espaces vectoriels de E, alors il existe des sous-espaces vectoriels $G_1, \dots, G_n$ tels que pour tout $i \in [\![1, n]\!]$, $G_i \subset F_i$ et $\sum\limits_{i=1}^{n} F_i = \bigoplus\limits_{i=1}^{n} G_i$ ».

- Pour $n = 1$, $\mathcal{P}_1$ est vraie (il suffit de prendre $G_1 = F_1$ et il n'y a rien d'autre à démontrer).
- Soit $n \in \mathbb{N}^*$. On suppose $\mathcal{P}_n$ vraie.

  Soit $F_1, \dots, F_n, F_{n+1}$ des sous-espaces vectoriels de E. On pose $F = \sum\limits_{i=1}^{n} F_i$.
  On note G_{n+1} un supplémentaire de $F \cap F_{n+1}$ dans F_{n+1}.
  Par définition, on a $G_{n+1} \subset F_{n+1}$ et $F_{n+1} = \left(F \cap F_{n+1}\right) \oplus G_{n+1}$.
  On va montrer que $F \oplus G_{n+1} = F + F_{n+1}$.
  - ***La somme $F + G_{n+1}$ est directe***
    Soit $x \in F \cap G_{n+1}$. G_{n+1} étant un sous-espace de F_{n+1}, on a $x \in F_{n+1}$. Donc $x \in F \cap F_{n+1}$ et $x \in G_{n+1}$. Donc $x = 0$ car $F \cap F_{n+1}$ et G_{n+1} sont en somme directe.
    Donc la somme de F et de G_{n+1} est directe.
  - ***Les espaces $F + G_{n+1}$ et $F + F_{n+1}$ sont égaux***
    On a $F + F_{n+1} = F + (F \cap F_{n+1}) + G_{n+1}$. Or $F \cap F_{n+1}$ étant un sous-espace vectoriel de F, on a $F + (F \cap F_{n+1}) = F$. Donc $F + F_{n+1} = F + G_{n+1}$.

  On a ainsi $G_{n+1} \subset F_{n+1}$ et $F \oplus G_{n+1} = F + F_{n+1}$.
  D'après $\mathcal{P}_n$, on peut choisir des sous-espaces vectoriels $G_1, G_2, \dots, G_n$ tels que pour tout $i \in [\![1, n]\!]$, $G_i \subset F_i$ et $\sum\limits_{i=1}^{n} F_i = \bigoplus\limits_{i=1}^{n} G_i$.
  On a ainsi

$$\forall i \in [\![1, n+1]\!], \quad G_i \subset F_i \quad \text{et} \quad \sum_{i=1}^{n+1} F_i = \left(\bigoplus_{i=1}^{n} G_i\right) \oplus G_{n+1} = \bigoplus_{i=1}^{n+1} G_i.$$

  Donc $\mathcal{P}_{n+1}$ est vraie.

On a montré par récurrence que pour tout $n \in \mathbb{N}^*$, $\mathcal{P}_n$ est vraie.
En particulier si $E = F_1 + \cdots + F_n$, il existe des sous-espaces vectoriels $G_1, \dots, G_n$ tels que :

$$\forall i \in [\![1, n]\!], \quad G_i \subset F_i \quad \text{et} \quad E = \bigoplus_{i=1}^{n} G_i.$$

Matrices, déterminants (révisions) 4

Exercices axés sur le calcul

Exercice 1 On pose $A = \begin{pmatrix} 13 & -8 & -12 \\ 12 & -7 & -12 \\ 6 & -4 & -5 \end{pmatrix}$.

1) À l'aide de la méthode du pivot, montrer que A est inversible et calculer son inverse A^{-1}.
Que remarque-t-on concernant A^{-1} ?

2) En déduire A^n pour tout $n \in \mathbb{Z}$.

Exercice 2

Soit a, b et c trois réels et M la matrice suivante :

$$M = \begin{pmatrix} 1+a & 1 & 1 \\ 1 & 1+b & 1 \\ 1 & 1 & 1+c \end{pmatrix}.$$

1) Calculer le déterminant de M.

2) Quand M est inversible, préciser son inverse.

Exercice 3

Calculer, sans machine, les déterminants des matrices suivantes et préciser si elles sont ou non inversibles.

1) $A = \begin{pmatrix} 1 & \sqrt[3]{2} & \sqrt[3]{4} \\ \sqrt[3]{4} & 1 & \sqrt[3]{2} \\ \sqrt[3]{2} & \sqrt[3]{4} & 1 \end{pmatrix}$ 2) $B = \begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{3} \\ \frac{1}{2} & \frac{1}{3} & \frac{1}{4} \\ \frac{1}{3} & \frac{1}{4} & \frac{1}{5} \end{pmatrix}$ 3) $C = \begin{pmatrix} 144 & 121 & 100 \\ 36 & 33 & 30 \\ 96 & 99 & 90 \end{pmatrix}$

Exercice 4

Soit a, b et c trois complexes. On pose $A = \begin{pmatrix} a & b & c \\ b & c & a \\ c & a & b \end{pmatrix}$.

1) Calculer $\det(A)$ par la formule développée.

2) Calculer $\det(A)$ en commençant par l'opération $L_1 \leftarrow L_1 + L_2 + L_3$.

Exercice 5 *Matrices « tridiagonales »*

Pour $n \in \mathbb{N} \setminus \{0, 1\}$, on considère le déterminant carré d'ordre n suivant :

$$\Delta_n = \begin{vmatrix} 3 & 1 & 0 & \cdots & 0 \\ 2 & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & 1 \\ 0 & \cdots & 0 & 2 & 3 \end{vmatrix}$$

Donner une relation entre Δ_{n+2}, Δ_{n+1} et Δ_n.
Puis déterminer Δ_n en fonction de n.

Exercice 6 ⋆

Soit $n \in \mathbb{N}^*$ et A_n la matrice carrée d'ordre n définie par $A_n = \big(\max(i, j)\big)_{1 \leqslant i, j \leqslant n}$.

Calculer $\det(A_n)$ en fonction de n.

Exercice 7 *Exponentielle d'une matrice nilpotente*

Soit $n \in \mathbb{N}^*$ et $A \in \mathcal{M}_n(\mathbb{C})$ une matrice nilpotente. On pose $\exp(A) = \sum_{k=0}^{n-1} \frac{1}{k!} A^k$.

Montrer que $\lim_{p \to \infty} \left(I_n + \frac{1}{p} A\right)^p = \exp(A)$.

Exercices axés sur le raisonnement

Exercice 8

Soit f l'endomorphisme de $\mathbb{R}^3$ canoniquement associé à la matrice :

$$M = \begin{pmatrix} 1 & 1 & -1 \\ -3 & -3 & 3 \\ -2 & -2 & 2 \end{pmatrix}.$$

1) Déterminer une base de $\mathrm{Ker}(f)$.

2) Déterminer une base de $\mathrm{Im}(f)$.

MP/MP*

Colles de **mathématiques**

Cet ouvrage s'adresse aux étudiants de deuxième année de **CPGE scientifiques MP/MP***.

La spécificité de ces classes est les interrogations orales ou colles. Elles participent grandement aux progrès des étudiants. Cependant, cette seconde année est courte. À l'assimilation régulière du cours s'ajoute l'aspect de l'entraînement à l'oral.

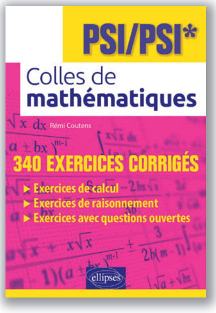
Dans l'objectif d'une préparation efficace, les **550 exercices** de ce livre sont classés en 3 catégories :

- **Les exercices de calcul**. Souvent application quasiment directe du cours, ils ont pour objectif, via la pratique calculatoire, de vérifier la connaissance et la compréhension des notions du cours.
- **Les exercices de raisonnement**. Ces exercices demandant plus de recul, leur objectif est de renforcer l'assimilation des concepts.
- **Les exercices avec questions ouvertes**. Ces exercices amènent l'étudiant à avoir sa propre réflexion, à construire sa démonstration ou son contre-exemple selon les cas.

Ces exercices ont été choisis pour leur approche formateur plutôt que leur originalité ou leur difficulté. Néanmoins certains énoncés, signalés par une ou deux étoiles, sont d'un niveau plus élevé.

Chaque exercice est **entièrement corrigé** parfois de plusieurs manières.

Dans la même collection :



www.editions-ellipses.fr
9 782340 040274